SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console ヘルプ

製品バージョン: 5.5

目次

1 Sophos Enterprise Console について

Sophos Enterprise Console は、Windows、Mac OS X、Linux、UNIX 環境のほか、VMware vShield を使用した仮想環境にインストールされているソフォスのセキュリティ製品を一元的に管理・アップデートする単一の管理コンソールです。

Enterprise Console の主な機能は次のとおりです。

- マルウェア、危険なファイルタイプや Web サイト、悪質なネットワークトラフィック、さらにアドウェアや他の不要と思われるアプリケーションからネットワークを保護する。
- ユーザーがアクセスできる Web サイトをコントロール。ネットワークをさらにマルウェアから保護し、ユーザーが不適切な Web サイトにアクセスすることを阻止する。
- ネットワーク上のアプリケーションの起動許可をコントロールする。
- クライアントファイアウォールによる各エンドポイントコンピュータの保護を集中管理する。
- コンピュータにインストールされていないパッチの評価を行う。
- 誤って機密情報を転送してしまうなど、過失によるエンドポイントからのデータ流出事故を削減する。
- エンドポイントにおける、未認証の外部ストレージデバイスや、無線接続機器の使用を防止する。
- ユーザーによる、ソフォスのセキュリティソフトの設定変更、無効化、またはアンインストールを防止する。

注
一部のライセンスには含まれていない機能もあります。利用するには追加購入が必要となります。使用可能なライセンスの詳細は、www.sophos.com/ja-jp/products/enduser-protection-suites/how-to-buy.aspx および www.sophos.com/ja-jp/products/server-security/how-to-buy.aspx を参照してください。

2 Enterprise Console の GUI の説明

2.1 GUI のレイアウト

Enterprise Console のユーザーインターフェースは、次の領域から構成されています。

ツールバー

ツールバーには、ソフォスのセキュリティソフトの使用・設定に最もよく使われるコマンドへのショートカットがあります。

詳細は、ツールバー ボタン (p. 2)を参照してください。

ダッシュボード

「**ダッシュボード**」には、ネットワークのセキュリティ ステータスが一目でわかるよう表示されます。

詳細は、ダッシュボードのパネル (p. 4)を参照してください。

コンピュータのリスト

コンピュータのリストは、右下に表示されます。次の 2種類のビューがあります。

- 「**エンドポイント**」ビューには、画面左下の「**グループ**」ペインで選択したグループ内のコンピュータが表示されます。詳細は、「エンドポイント」ビューについて (p. 6)を参照してください。
- 「**アップデートマネージャ**」ビューには、Sophos Update Manager がインストールされているコンピュータが表示されます。詳細は、「アップデートマネージャ」ビューについて (p. 10)を参照してください。

2.2 ツールバー ボタン

ツールバー ボタンの説明は次の表を参照してください。ツールバー ボタンのなかには、特定の状況下のみで使用できるものもあります。たとえば、ウイルス対策ソフトやファイアウォールソフトをインストールする「**保護**」ボタンは、「**エンドポイント**」ビューの「**グループ**」ペインで、コンピュータのグループを選択している場合のみ使用できます。

ツールバーボタン	説明	注
	**コンピュータの検出**	ネットワーク上のコンピュータを検出し、コンソールに追加する。 詳細は、ネットワーク上のコンピュータを検出する (p. 33)を参照してください。
	**グループの作成**	コンピュータの新規グループを作成する。 詳細は、グループを作成する (p. 24)を参照してください。
	**ポリシーの表示/編集**	「**ポリシー**」ペインで選択したポリシーを開き、編集する。 詳細は、ポリシーを編集する (p. 31)を参照してください。
	**保護**	コンピュータのリストで選択したコンピュータに、ウイルス対策ソフトやファイアウォールソフトをインストールする。 詳細は、コンピュータを自動保護する (p. 45)を参照してください。
	**エンドポイント**	コンピュータのリストで「**エンドポイント**」ビューに切り替える。 「**エンドポイント**」ビューには、「**グループ**」ペインで選択したグループのコンピュータが表示されます。 詳細は、「エンドポイント」ビューについて (p. 6)を参照してください。
	**アップデートマネージャ**	コンピュータのリストで「**アップデートマネージャ**」ビューに切り替える。 「**アップデートマネージャ**」ビューには、Sophos Update Manager がインストールされているコンピュータが表示されます。 詳細は、「アップデートマネージャ」ビューについて (p. 10)を参照してください。
	**ダッシュボード**	「**ダッシュボード**」を表示/非表示にする。 「**ダッシュボード**」には、ネットワークのセキュリティ ステータスが一目でわかるよう表示されます。 詳細は、ダッシュボードのパネル (p. 4)を参照してください。
	**レポート**	「**レポートマネージャ**」を開き、ネットワークで発生した警告やイベントに関するレポートを作成する。 詳細は、レポートの作成 (p. 210)を参照してください。

ツールバーボタン	説明	注
	**Sophos Central**	Sophos Central を開く。 Sophos Central の詳細は、サポートデータベースの文章 119598 を参照してください。Sophos Central へ移行する方法については、サポートデータベースの文章 122264 を参照してください。
	**Sophos Mobile**	Sophos Mobile の URL が設定されている場合は、Sophos Mobile の Web コンソールが開く。これは、スマートフォンやタブレット端末上のアプリやセキュリティ設定を管理する、MDM (モバイルデバイス管理) ソリューションです。 詳細は、Sophos Mobile の URL を設定する (p. 43)を参照してください。

2.3 ダッシュボードのパネル

ダッシュボードに含まれるパネルは次のとおりです。

ダッシュボードのパネル	説明
コンピュータ	ネットワーク上のコンピュータの総数のほか、接続されているコンピュータ、管理対象コンピュータ、管理対象外のコンピュータの台数が表示されます。 管理対象コンピュータ、管理対象外のコンピュータ、接続されているコンピュータ、またはすべてのコンピュータの一覧を表示するには、「**コンピュータ**」パネル内の各リンクをクリックします。
アップデート	アップデートマネージャのステータスが表示されます。
警告を発したコンピュータ	管理対象コンピュータのうち、次のようなアイテム/イベントに関する警告を発したものの数と、その割合が表示されます。 • 既知/未知のウイルス/スパイウェア • 疑わしい動作/ファイル • アドウェアや他の不要と思われるアプリケーション 管理対象コンピュータのうち、未対処の警告があるものの一覧を表示するには、パネルのタイトル「**警告を発したコンピュータ**」をクリックします。

ダッシュボードのパネル	説明
設定レベルを超過するイベントのあるコンピュータ	過去 1週間で、しきい値を超える数のイベントが発生したコンピュータの台数が表示されます。 デバイスコントロール、データコントロール、アプリケーション コントロール、またはファイアウォールに関するイベントが発生したコンピュータの一覧を表示するには、「**設定レベルを超過するイベントのあるコンピュータ**」パネル内の各リンクをクリックします。 **注** ライセンスによって、一部のイベントタイプは表示されない場合があります。
ポリシー	管理対象コンピュータのうち、グループポリシーに違反しているものや、ポリシーの比較でエラーが発生したもの数と、その割合が表示されます。また、コンソールから送信されたポリシーの変更内容に対応済みでないコンピュータも含まれています。 管理対象コンピュータのうち、ポリシーと異なるものの一覧を表示するには、パネルのタイトル「**ポリシー**」をクリックします。
保護	接続されている管理対象コンピュータのうち、最新版の Sophos Endpoint Security and Control または Sophos Anti-Virus がインストールされていないものや、不明な検出データを使用しているものの数と、その割合が表示されます。 接続されている管理対象コンピュータのうち、最新版が適用されていないものの一覧を表示するには、パネルのタイトル「**保護**」をクリックします。
エラー	管理対象コンピュータのうち、検索、アップデート、またはファイアウォールに関する未対処のエラーがあるものの数と、その割合が表示されます。 管理対象コンピュータのうち、未対処のソフォス製品エラーが発生しているものの一覧を表示するには、パネルのタイトル「**エラー**」をクリックします。

2.4 セキュリティ ステータス アイコン

ダッシュボードと Enterprise Console のステータスバーに表示されるセキュリティ ステータス アイコンの説明は次の表を参照してください。

セキュリティ ステータス アイコン	説明
	**正常** 問題のあるコンピュータの割合は、警報レベル未満です。
	**警告** 問題のあるコンピュータの割合は、警報レベルを超えています。

セキュリティ ステータス アイコン	説明
	**緊急** 問題のあるコンピュータの割合は、緊急レベルを超えています。

ダッシュボードパネルのセキュリティ ステータス アイコン

ダッシュボードパネルのセキュリティ ステータス アイコンは、各ダッシュボードパネルの右上部に表示されます。各パネルで扱われている特定のセキュリティエリアの状態を示します。

ダッシュボードパネルのセキュリティ ステータス アイコンには、各パネル内のアイコンで最も深刻なレベルが表示されます。

- パネルのセキュリティ ステータス アイコンは、パネル内の少なくとも 1つのアイコンが「警報」レベルになると、「**正常**」から「**警報**」に変わります。
- パネルのセキュリティ ステータス アイコンは、パネル内の少なくとも 1つのアイコンが「緊急」レベルになると、「**警報**」から「**緊急**」に変わります。

ネットワーク全体のセキュリティ ステータス アイコン

ネットワーク全体のセキュリティ ステータス アイコンは、Enterprise Console ステータスバーの右端に表示されます。ネットワーク全体のセキュリティ状態を示します。

ネットワーク全体のセキュリティ ステータス アイコンには、**ダッシュボード**パネルのアイコンで最も深刻なレベルが表示されます。

- ネットワーク全体のセキュリティ ステータス アイコンは、ダッシュボード上の少なくとも 1つのアイコンが「警報」レベルになると、「**正常**」から「**警報**」に変わります。
- ネットワーク全体のセキュリティ ステータス アイコンは、**ダッシュボード**上の少なくとも 1つのアイコンが「緊急」レベルになると、「**警報**」から「**緊急**」に変わります。

Enterprise Console をはじめてインストールまたはアップグレードする際、デフォルトの警報・緊急レベルが**ダッシュボード**に適用されます。警報・緊急レベルを任意に設定する方法は、ダッシュボードのパネル (p. 4)を参照してください。

また、各**ダッシュボード**パネルで警報・緊急レベルになった場合、特定の宛先にメール警告を送信するよう設定できます。手順については、ネットワークステータスのメール警告を設定する (p. 196)を参照してください。

2.5 「エンドポイント」ビューについて

コンピュータのリスト

「**エンドポイント**」ビューで、コンピュータのリストに、「**グループ**」ペインで選択したグループ内のエンドポイントコンピュータが表示されます。

このビューには複数のタブがあります。「**ステータス**」タブには、コンピュータがオンアクセス検索で保護されているか、グループポリシーに準拠しているか、どの機能が有効になっているか、およびソフトウェアが最新版であるかが表示されます。また、このタブには警告の有無も表示されます。その他のタブをクリックすると、各項目に関する詳細が表示されます。

コンピュータのリストは、「**表示**」フィルタを使用してフィルタリングすることができます。「**表示**」ドロップダウンリストで、表示するコンピュータを選択します。たとえば、問題のあるコンピュータを表示するには、「**問題があると思われるコンピュータ**」を選択します。

コンピュータのリストは、この他に、マルウェア、不要と思われるアプリケーション、または疑わしいファイルなどの検出項目名でフィルタリングすることもできます。詳細は、検出アイテム名でコンピュータをフィルタリングする (p. 9)を参照してください。

コンピュータは、コンピュータ名、コンピュータの説明、または IP アドレスを使って検索できます。詳細は、Enterprise Console でコンピュータを検索する (p. 9)を参照してください。

コンピュータのリストに表示されるアイコンの説明は、コンピュータのリストのアイコン (p. 7)を参照してください。

コンピュータのリストに表示される情報は、コピーしたり印刷したりすることができます。詳細は、コンピュータのリストのデータをコピーする (p. 221)およびコンピュータのリストのデータを印刷する (p. 221)を参照してください。

「グループ」ペイン

「**グループ**」ペインでは、グループ

を作成し、ネットワーク上のコンピュータを配置します。グループは手動で作成するか、または Active Directory のコンテナを (コンピュータの有無に関わらず) インポートすることができます。インポートしたコンテナを Enterprise Console のコンピュータのグループとして使います。

詳細は、グループを作成、使用する (p. 23)を参照してください。

「**グループ外のコンピュータ**」フォルダ

は、作成したグループに配置されていないコンピュータ用のフォルダです。

「ポリシー」ペイン

「**ポリシー**」ペインでは、コンピュータのグループに適用するポリシーを作成・設定します。詳細は、ポリシーを作成、使用する (p. 26)を参照してください。

2.6 コンピュータのリストのアイコン

警告

アイコン	説明
	赤い警告アイコンが「**ステータス**」タブの「**警告とエラー**」カラムに表示された場合は、ウイルス、ワーム、トロイの木馬、スパイウェア、または疑わしい動作が検出・検知されたことを意味します。

アイコン	説明
	黄色い警告アイコンが「**ステータス**」タブの「**警告とエラー**」カラムに表示された場合は、次のいずれか 1つの問題が発生したことを意味します。 • 疑わしいファイルが検出された。 • アドウェアやその他の不要と思われるアプリケーションが検出された。 • エラーが発生した。 黄色い警告アイコンが「**ポリシーコンプライアンス**」カラムに表示された場合は、グループ内の他のコンピュータと異なるポリシー (複数の場合もあります) が適用されていることを意味します。

コンピュータに複数の警告やエラーがある場合は、優先順位が最も高い警告のアイコンが「**警告とエラー**」カラムに表示されます。警告タイプの優先順位は以下のとおりです (降順)。

1. ウイルス/スパイウェア警告
2. 疑わしい動作警告
3. 疑わしいファイル警告
4. アドウェア/不要と思われるアプリケーション警告
5. ソフトウェアのアプリケーションエラー (インストールエラーなど)

コンピュータに優先順位が同じ警告が複数ある場合は、最も新しい警告がコンピュータのリストに表示されます。

保護が無効、または最新でない

「**ステータス**」タブの各機能の「ステータス」カラムにグレーの機能アイコンが表示された場合は、その機能が無効になっていることを意味します。たとえば、「**オンアクセス**」カラムにグレーの盾アイコン

が表示された場合は、オンアクセス検索が非アクティブなことを意味します。

「**更新状況**」カラムに、時計アイコン

が表示された場合は、セキュリティ対策ソフトが最新版でないことを意味します。

コンピュータのステータス

アイコン	説明
	緑色のコネクタが付いているコンピュータ アイコンは、コンピュータが Enterprise Console によって管理されていることを意味します。
	黄色い砂時計が付いているコンピュータ アイコンは、セキュリティ対策ソフトのインストールが保留状態であることを意味します。
	黄色い下向き矢印が付いているコンピュータ アイコンは、セキュリティ対策ソフトのインストールが進行中であることを意味します。

アイコン	説明
	グレーのコンピュータ アイコンは、コンピュータが Enterprise Console によって管理されていないことを意味します。
	赤い×印が付いているコンピュータ アイコンは、通常、Enterprise Console によって管理されているコンピュータがネットワークから切断されたことを意味します。(管理対象外のコンピュータで、接続されていないものは表示されません。)

2.7 検出アイテム名でコンピュータをフィルタリングする

コンピュータのリストは、マルウェア、不要と思われるアプリケーション、または疑わしいファイルなどの検出アイテム名でフィルタリングできます。これには、「管理対象コンピュータ: 次のアイテムに感染 -...」フィルタを設定します。指定したフィルタは、他のコンピュータリストのフィルタと共に、「**表示**」ドロップダウンリストに表示されます。

フィルタの設定方法は次のとおりです。

1. 「**ツール**」メニューで、「**フィルタの環境設定**」をクリックします。
2. 「**コンピュータリストのフィルタの環境設定**」ダイアログボックスで、フィルタリングする検出アイテムの名前を入力します。ネットワークで検出されたアイテムのアイテム名は、次のいずれかの方法で参照できます。
   - 「コンピュータのリスト」ビュー: 「 **警告とエラーの詳細**」タブの「**検出されたアイテム**」カラム。

     コンピュータで複数のアイテムが検出された場合は、「**検出されたアイテム**」カラムに最も日付が新しく、最も優先順位の高いアイテムのうち、最も日付が新しいもののみが表示されるため、フィルタリングの対象にするアイテムが表示されない場合があります。
   - 「**警告とエラーの対処**」ダイアログボックス。ダイアログボックスを開くには、コンピュータのリストからコンピュータを選択するか、「**グループ**」ペインでコンピュータのグループを選択して、右クリックして「**警告とエラーの対処**」をクリックします。
   - 「**コンピュータの詳細**」ダイアログボックス。ダイアログボックスを開くには、感染したコンピュータをダブルクリックします。そして、スクロールダウンして「**未対処の警告とエラー**」セクションを表示します。
   - 「**レポート**」(例: 「**警告のサマリー**」や「**警告とイベント - アイテム名ごと**」など): 「**レポート マネージャ**」を開くには、「**ツール**」メニューで「**レポートの管理**」をクリックします。

   ワイルドカード文字を使用できます。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。例えば、「Mal*」と入力し、フィルタを適用すると、コンピュータのリストの画面には、「Mal/Conficker-A」や「Mal/Packer」など「Mal」ではじまる名前を持つマルウェアに感染したコンピュータが表示されます。

2.8 Enterprise Console でコンピュータを検索する

次のいずれかの条件を指定して、Enterprise Console でコンピュータを検索できます。

- コンピュータ名
- コンピュータの説明
- IP アドレス

1. コンピュータを検索するには、以下の操作のいずれかの手順を実行してください。
   - 「CTRL+F」を押します。
   - 「**編集**」メニューで、「**コンピュータの検索**」をクリックします。
   - コンピュータのリスト内で任意の場所を右クリックして、「**コンピュータの検索**」をクリックします。
2. 「**検索**」ダイアログボックスで、検索条件を入力します。

   「**検索する文字列**」フィールドで、大文字と小文字は区別されません。文字列の終わりには、ワイルドカード文字があるとして処理されるので、指定する必要はありません。

   ワイルドカード文字「*」、および「?」を使用できます。

   例:

検索の条件	検索結果
UKlapt	「uklapt」ではじまる文字列を検索。例: UKlaptop-011、UKlaptop-155、uklaptop132。
Ukla*	「ukla」ではじまる文字列を検索。ワイルドカード文字は、文字列の終わりにあるとして処理されるので、指定する必要はありません。検索結果は、「UKlapt」と同じです。例: UKlaptop-011、UKlaptop-155、uklaptop132。
***ukla**	「ukla」を含む文字列を検索。例: UKlaptop-011、055uklax、056-Dukla-sales。
Ukl*t	「ukl」ではじまり、「t」を含み、任意の文字で終わる文字列を検索。例: UKlaptop-011、ukLite55。
?klap	任意の 1文字の後に「klap」が続き、任意の文字で終わる文字列を検索。例: UKlaptop-011、uklapland33。
UKl??t	「ukl」ではじまり、任意の 2文字の後に「t」が続き、任意の文字で終わる文字列を検索。例: UKlaptop-011、uklist101。

2.9 「アップデートマネージャ」ビューについて

コンピュータのリスト

「**アップデートマネージャ**」ビューでは、ソフォスのセキュリティソフトの自動アップデート (ソフォス Web サイト経由) を設定したり、アップデートマネージャのステータスや詳細を表示できます。

コンピュータのリストには、Sophos Update Manager がインストールされているコンピュータが表示されます。

ソフトウェアのサブスクリプション

「**ソフトウェアのサブスクリプション**」ペインでは、ソフトウェアのサブスクリプションを追加または編集し、ソフォスのサーバーからエンドポイントにダウンロードする、各プラットフォーム版のソフトウェアのバージョンを指定します。

3 Sophos Enterprise Console の使い方

ネットワークを保護するためには、Enterprise Console のインストールと、「**セキュリティソフトのダウンロード**」ウィザードを完了した後に、いくつかのタスクを実行する必要があります。ここでは、そのタスクの概要について説明します。Enterprise Console の使い方について、詳しくは、後述の関連するセクションやドキュメントを参照してください。

ソフォスのセキュリティソフトの使用や管理に関するベストプラクティスについて、「Sophos Enterprise Console ポリシー設定ガイド」を参照することを推奨します。ソフォスの製品ドキュメントは次のサイトから入手可能です。 http://www.sophos.com/ja-jp/support/documentation

「**セキュリティソフトのダウンロード**」ウィザードを完了していない場合は、「セキュリティソフトのダウンロード」ウィザードを起動する (p. 68)を参照してください。

ネットワークを保護するには、次のステップを実行してください。

1. **グループを作成する。**

   グループは手動で個別に作成するか、または Active Directory のコンテナを (コンピュータの有無に関わらず) インポートすることができます。インポートしたコンテナを Enterprise Console のコンピュータのグループとして使います。

   Active Directory のコンテナをインポートする場合は、Active Directory からコンテナやコンピュータをインポートする (p. 33)を参照してください。はじめに、Active Directory からコンピュータなしでコンテナをインポートし、次に、Active Directory とグループを同期するなどの方法で、グループにコンピュータを追加することを推奨します。

   グループを手動で作成する方法の詳細は、グループを作成、使用する (p. 23)を参照してください。
2. **ポリシーを設定する。**

   Enterprise Console には、ネットワークの保護に必要な一連のデフォルトポリシーが用意されています。デフォルトの**アップデート**ポリシーと**ウイルス対策および HIPS** ポリシーは、ソフトウェアのインストール完了後、そのまますぐ使えます。ファイアウォール ポリシーを設定するには、「**ファイアウォール ポリシー**」ウィザードを使用してください。詳細は、基本的なファイアウォールポリシーを設定する (p. 113)を参照してください。
3. **ネットワーク上のコンピュータを検出し、コンソールに追加する。**

   ステップ 1 で Active Directory からコンテナやコンピュータをインポートした場合、ここでの手順は必要ありません。それ以外の場合は、ネットワーク上のコンピュータを検出する (p. 33)を参照してください。
4. **コンピュータを保護する。**

   ネットワーク上のコンピュータの保護は、次の 2とおりの方法から最も適したものを選択できます。

   - **「コンピュータの保護 ウィザード」を使用する**

     「**グループ外のコンピュータ**」フォルダからコンピュータを別のグループにドラッグ & ドロップすると、ウィザードが起動するので、指示に従ってコンピュータを保護してください。詳細は、コンピュータを自動保護する (p. 45)を参照してください。

   - **Active Directory と同期中、コンピュータを自動保護する**

     Active Directory との同期を選択した場合、Windows コンピュータの自動保護も選択できます。これは、「**Active Directory の同期 ウィザード**」または「**同期のプロパティ**」ダイアログボックスにて指定できます。手順については、同期を利用してコンピュータを自動的に保護する (p. 40)を参照してください。
5. **コンピュータが保護されていることを確認する。**

インストールが完了したら、新規グループのコンピュータの一覧を再確認します。「**オンアクセス**」カラムに「アクティブ」という表示があれば、コンピュータはオンアクセス検索で保護され、Enterprise Console によって管理されています。詳細は、ネットワークが保護されているか確認する (p. 47)を参照してください。

6. **コンピュータをクリーンアップする。**

   ネットワーク上で、ウイルス、不要と思われるアプリケーション、またはその他の問題が検出された場合は、コンピュータを直ちにクリーンアップする (p. 54)の説明に従って、該当するコンピュータをクリーンアップしてください。

追加の保護オプション

デフォルトで Sophos Endpoint Security and Control は、マルウェア (ウイルス、トロイの木馬、ワーム、スパイウェア)、アドウェアやその他の不要と思われるアプリケーション、疑わしい動作、および悪質なネットワークトラフィックを検出します。また、マルウェア感染サイトへのアクセスをブロックし、インターネットからダウンロードしたコンテンツも検索します。これ以外のセキュリティや生産性に関する機能を有効にすることもできます。詳細はグループを作成、使用する (p. 23)を参照してください。

管理オプション

Enterprise Console では、複数のロールを設定して権限を追加し、Windows のユーザーやグループをロールに追加できます。システム管理者ロールには、Sophos Full Administrators という Windows のグループが含まれています。このロールはフル権限を持っており、初期設定は必要ありません。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

IT 資産はサブ管理サイトとして分割できます。作成したサブ管理サイトには、Enterprise Console のコンピュータのグループを追加できます。そして、Windows のユーザーやグループをサブ管理サイトに追加し、サブ管理サイトへのアクセスをコントロールできます。「**デフォルト**」サブ管理サイトには、「**グループ外のコンピュータ**」を含む、Enterprise Console のグループがすべて含まれます。サブ管理サイトの詳細はロールとサブ管理サイトを管理する (p. 14)を参照してください。

ヒント
YouTube チャンネル、SophosGlobalSupport の Sophos Enduser Protection より、Enterprise Console の設定方法や使い方を解説する動画を視聴できます。

4 Enterprise Console の設定

4.1 ロールとサブ管理サイトを管理する

重要
ロールベースの管理を既に利用している場合、ロールとサブ管理サイトを設定するには、「**ロールベースの管理**」権限が必要です。システム管理者ロールには、Sophos Full Administrators という Windows のグループが含まれています。このロールはフル権限を持っており、初期設定は必要ありません。詳細は、事前定義済みのロールとは？ (p. 15)および権限と実行できるタスクについて (p. 18)を参照してください。

複数のロールを設定して権限を追加し、Windows のユーザーやグループに付与すると、コンソールへのアクセスをロールベースで管理できます。たとえば、ヘルプデスク担当者は、コンピュータのアップデートやクリーンアップを実行できますが、ポリシー設定の権限は与えられていません。ポリシーの設定は、管理者ロールの役割です。

Enterprise Console を開くには、Sophos Console Administrators グループのメンバーである必要があります。また、そのユーザーを少なくとも 1つの Enterprise Console のロールと、サブ管理サイトに追加する必要があります。Sophos Full Administrators グループに所属するユーザーには、Enterprise Console に対するフルアクセス権限が付与されています。

注
リモートや追加の Enterprise Console の使用をユーザーに許可するには、新しい Enterprise Console ユーザーを追加する (p. 22)を参照してください。

ロールは、独自のものを作成したり、あらかじめ定義されているものを使用できます。

個別のユーザー、またはユーザーが所属する Windows グループをロールに追加することで、一人のユーザーを任意の数のロールに追加できます。

コンソールの特定のタスクに対する実行権限が与えられていない場合でも、ユーザーはタスクの設定内容を表示できます。どのロールにも追加されていないユーザーは、Enterprise Console を開くことができません。

また、ユーザーが操作を実行できるコンピュータやグループを制限することもできます。IT 資産はサブ管理サイトとして分割できます。作成したサブ管理サイトには、Enterprise Console のコンピュータのグループを追加できます。そして、Windows のユーザーやグループをサブ管理サイトに追加し、サブ管理サイトへのアクセスをコントロールできます。「**デフォルト**」サブ管理サイトには、「**グループ外のコンピュータ**」を含む、Enterprise Console のグループがすべて含まれます。

ユーザーは、自分が割り当てられているサブ管理サイトだけ表示できます。複数のサブ管理サイトに追加されている場合、ユーザーは表示するサブ管理サイトを選択できます。一度に表示できるサブ管理サイトの数は 1つです。Enterprise Console で開いているサブ管理サイトが、アクティブなサブ管理サイトです。各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

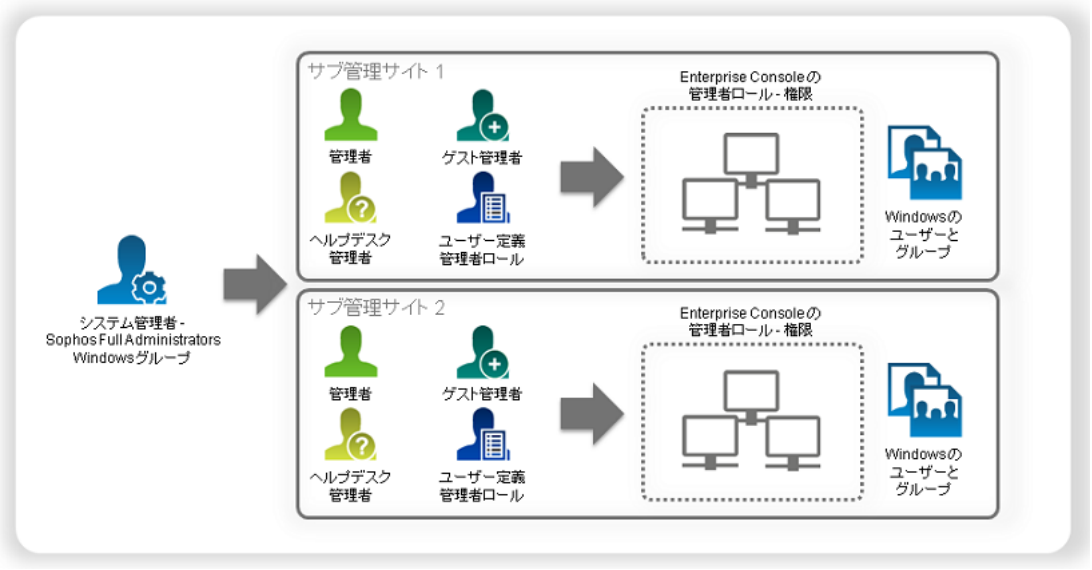


図 1：ロールとサブ管理サイト

4.1.1 事前定義済みのロールとは？

Enterprise Console には、次の 4種類のロールがあらかじめ設定されています。

ロール	説明
システム管理者	ネットワーク上のソフォスのセキュリティソフト、および Enterprise Console のロールを管理するために、あらかじめ設定されているロール。フルコントロール権限が与えられています。システム管理者ロールは、編集も削除もできません。
管理者	ネットワーク上のソフォスのセキュリティソフトを管理するために、あらかじめ設定されているロール。ただし、Enterprise Console のロールは管理できません。管理者ロールは、名前の変更、編集、および削除ができます。
ヘルプデスク	クリーンアップ、コンピュータのアップデートなど、修復権限だけを持つロール。あらかじめ設定されています。ヘルプデスクロールは、名前の変更、編集、および削除ができます。
ゲスト	読み取り専用で Enterprise Console を開けるロール。あらかじめ設定されています。ゲストロールは、名前の変更、編集、および削除ができます。

管理者ロール、ヘルプデスクロール、ゲストロールを編集したり、または独自のロールを作成することができます (ロールを作成する (p. 15) を参照)。

4.1.2 ロールを作成する

ロールベースの管理を既に利用している場合、ここでのタスクを実行するには「**ロールベースの管理**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**ツール**」メニューで、「**ロールとサブ管理サイトの管理**」をクリックします。

2. 「**ロールとサブ管理サイトの管理**」ダイアログボックスの「**ロールの管理**」タブで、「**作成**」をクリックします。
   「**ロールの作成**」ダイアログボックスが表示されます。
3. 「**ロール名**」フィールドにロールの名前を入力します。
4. 「**権限**」ペインで、ロールに追加する権限 (複数可) を選択し、「**追加**」をクリックします。
5. 「**ユーザーとグループ**」ペインで「**追加**」をクリックします。
6. 「**ユーザーまたはグループの選択**」ダイアログボックスで、ロールに追加する Windows のユーザーまたはグループの名前を入力します。「**OK**」をクリックします。

   必要に応じて、ステップ 5～6 を繰り返して複数のユーザーやグループをロールに追加します。

4.1.3 ロールを削除する

ロールベースの管理を既に利用している場合、ここでのタスクを実行するには「**ロールベースの管理**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**ツール**」メニューで、「**ロールとサブ管理サイトの管理**」をクリックします。
2. 「**ロールとサブ管理サイトの管理**」ダイアログボックスの「**ロールの管理**」タブで、削除するロールを選択し、「**削除**」をクリックします。

注
あらかじめ定義されているシステム管理者ロールは削除できません。

4.1.4 ロールを編集する

ロールベースの管理を既に利用している場合、ここでのタスクを実行するには「**ロールベースの管理**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**ツール**」メニューで、「**ロールとサブ管理サイトの管理**」をクリックします。
2. 「**ロールとサブ管理サイトの管理**」ダイアログボックスの「**ロールの管理**」タブで、編集するロールを選択し、「**編集**」をクリックします。
   「**ロールの編集**」ダイアログボックスが表示されます。
3. 「**権限**」ペインで、適宜、権限をロールに追加、または既存の権限をロールから削除します。
4. 「**ユーザーとグループ**」ペインで、適宜、Windows のユーザーやグループをロールに追加、または既存のユーザーやグループをロールから削除します。

4.1.5 ロールに権限を付与する

ロールベースの管理を既に利用している場合、ここでのタスクを実行するには「**ロールベースの管理**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**ツール**」メニューで、「**ロールとサブ管理サイトの管理**」をクリックします。
2. 「**ロールとサブ管理サイトの管理**」ダイアログボックスの「**ロールの管理**」タブで、権限を追加するロールを選択し、「**編集**」をクリックします。
   「**ロールの編集**」ダイアログボックスが表示されます。
3. 「**権限**」ペインの「**利用可能な権限**」リストから権限を選択し、「**追加**」をクリックします。

4.1.6 サブ管理サイトを作成する

ロールベースの管理を既に利用している場合、ここでのタスクを実行するには「**ロールベースの管理**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**ツール**」メニューで、「**ロールとサブ管理サイトの管理**」をクリックします。
2. 「**ロールとサブ管理サイトの管理**」ダイアログボックスの「**サブ管理サイトの管理**」タブで、「**作成**」をクリックします。
   「**サブ管理サイトの作成**」ダイアログボックスが表示されます。
3. 「**サブ管理サイト名**」フィールドにサブ管理サイトの名前を入力します。
4. 「**Enterprise Console グループ**」ペインで、サブ管理サイトに追加するグループを選択します。
5. 「**ユーザーとグループ**」ペインで、「**追加**」をクリックし、Windows のユーザーやグループをサブ管理サイトに追加します。

4.1.7 アクティブなサブ管理サイトを変更する

複数のサブ管理サイトに所属しているユーザーは、Enterprise Console を開いたときに表示するサブ管理サイトを選択できます。または、Enterprise Console を開いているときに、サブ管理サイトの表示を切り替えられます。

一度に表示できるサブ管理サイトの数は 1つです。アクティブなサブ管理サイトを変更すると、Enterprise Console で選択したサブ管理サイトが読み込まれます。

アクティブなサブ管理サイトを変更する方法は次のとおりです。

1. 「**ツール**」メニューから「**アクティブなサブ管理サイトの選択**」を選択します。
2. 「**アクティブなサブ管理サイトの選択**」ダイアログボックスで、表示するサブ管理サイトを選択し、「**OK**」をクリックします。

4.1.8 サブ管理サイトを編集する

ロールベースの管理を既に利用している場合、ここでのタスクを実行するには「**ロールベースの管理**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**ツール**」メニューで、「**ロールとサブ管理サイトの管理**」をクリックします。
2. 「**ロールとサブ管理サイトの管理**」ダイアログボックスの「**サブ管理サイトの管理**」タブで、編集するサブ管理サイトを選択し、「**編集**」をクリックします。
3. 「**サブ管理サイトの編集**」ダイアログボックスで、必要に応じて、サブ管理サイトの名前、サブ管理サイトに含む Enterprise Console のグループ、またはサブ管理サイトへのアクセスを許可する Windows のユーザーやグループを変更します。「**OK**」をクリックします。

4.1.9 サブ管理サイトをコピーする

ロールベースの管理を既に利用している場合、ここでのタスクを実行するには「**ロールベースの管理**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**ツール**」メニューで、「**ロールとサブ管理サイトの管理**」をクリックします。
2. 「**ロールとサブ管理サイトの管理**」ダイアログボックスの「**サブ管理サイトの管理**」タブで、コピーするサブ管理サイトを選択し、「**コピー**」をクリックします。

複製したサブ管理サイトが一覧に表示されます。

3. 新しく作成したサブ管理サイトを選択し、「**編集**」をクリックします。サブ管理サイトの名前を変更します。必要に応じて、サブ管理サイトに含むコンピュータのグループや、サブ管理サイトへのアクセスを許可する Windows のユーザー/グループを変更します。

4.1.10 サブ管理サイトを削除する

ロールベースの管理を既に利用している場合、ここでのタスクを実行するには「**ロールベースの管理**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**ツール**」メニューで、「**ロールとサブ管理サイトの管理**」をクリックします。
2. 「**ロールとサブ管理サイトの管理**」ダイアログボックスの「**サブ管理サイトの管理**」タブで、削除するサブ管理サイトを選択し、「**削除**」をクリックします。

   「**デフォルト**」サブ管理サイトは削除できません。

4.1.11 ユーザーやグループのロール/サブ管理サイトを表示する

Windows のユーザーやグループが追加されている、ロールおよびサブ管理サイトを表示する方法は次のとおりです。

1. 「**ツール**」メニューで、「**ロールとサブ管理サイトの管理**」をクリックします。
2. 「**ロールとサブ管理サイトの管理**」ダイアログボックスで、「**ユーザーとグループの表示**」タブを開き、「**ユーザーやグループの選択**」ボタンをクリックします。
3. 「**ユーザーまたはグループの選択**」ダイアログボックスで、追加先のロールおよびサブ管理サイトを表示する、ユーザーまたはグループを選択し、「**OK**」をクリックします。

4.1.12 権限と実行できるタスクについて

注
ライセンスによって、一部の権限は適用できない場合があります。

権限	タスク
監査	監査の有効化、監査の無効化

権限	タスク
コンピュータの検索、保護およびグループ	検索の開始、検索の停止、ネットワークの検索を実行する際のドメインの検出、IP アドレス範囲を指定した検索、Active Directory の検索 Active Directory のコンピュータやグループのインポート、Active Directory のグループのインポート ファイルからのコンピュータ名のインポート コンピュータの削除 コンピュータの保護 グループと Active Directory の同期 グループの同期のプロパティの変更 グループの同期の削除 コンピュータの移動 グループの作成 グループ名の変更 グループの移動 グループの削除 グループへのポリシーの適用
データコントロール設定	データコントロールのルールの作成 データコントロールのルールの編集 データコントロールのルールのコピー データコントロールのルールの削除 データコントロールの対象からファイルを除外 コンテンツ コントロール リストの作成 コンテンツ コントロール リストの編集 コンテンツ コントロール リストのコピー コンテンツ コントロール リストの削除
データコントロールのイベント	データコントロールのイベントビューアの表示 コンピュータの詳細へのデータコントロールのイベントの表示
ポリシー設定 - ウイルス対策および HIPS	ウイルス対策および HIPS ポリシーの作成 ウイルス対策および HIPS ポリシーのコピー ウイルス対策および HIPS ポリシーの名前の変更 ウイルス対策および HIPS ポリシーの編集 ウイルス対策および HIPS の設定をデフォルトに戻す ウイルス対策および HIPS ポリシーの削除 脅威管理リストの項目の追加/削除

権限	タスク
ポリシー設定 - アプリケーションコントロール	アプリケーション コントロール ポリシーの作成 アプリケーション コントロール ポリシーのコピー アプリケーション コントロール ポリシーの名前の変更 アプリケーション コントロール ポリシーの編集 アプリケーション コントロールの設定をデフォルトに戻す アプリケーション コントロール ポリシーの削除
ポリシー設定 - データコントロール	データコントロール ポリシーの作成 データコントロール ポリシーのコピー データコントロール ポリシーの名前の変更 データコントロール ポリシーの編集 データコントロールの設定をデフォルトに戻す データコントロール ポリシーの削除
ポリシー設定 - デバイスコントロール	デバイスコントロール ポリシーの作成 デバイスコントロール ポリシーのコピー デバイスコントロール ポリシーの名前の変更 デバイスコントロール ポリシーの編集 デバイスコントロールの設定をデフォルトに戻す デバイスコントロール ポリシーの削除
ポリシー設定 - ファイアウォール	ファイアウォールポリシーの作成 ファイアウォールポリシーのコピー ファイアウォールポリシーの名前の変更 ファイアウォールポリシーの編集 ファイアウォールの設定をデフォルトに戻す ファイアウォールポリシーの削除
ポリシー設定 - パッチ	パッチポリシーの作成 パッチポリシーのコピー パッチポリシーの名前の変更 パッチポリシーの編集 パッチの設定をデフォルトに戻す パッチポリシーの削除

権限	タスク
ポリシー設定 - タンパー プロテクション	タンパー プロテクション ポリシーの作成 タンパー プロテクション ポリシーのコピー タンパー プロテクション ポリシーの名前の変更 タンパー プロテクション ポリシーの編集 タンパー プロテクションの設定をデフォルトに戻す タンパー プロテクション ポリシーの削除
ポリシー設定 - アップデート	アップデートポリシーの作成 アップデートポリシーのコピー アップデートポリシーの名前を変更 アップデートポリシーの編集 アップデートの設定をデフォルトに戻す アップデートポリシーの削除 サブスクリプションの作成 サブスクリプションの編集 サブスクリプション名の変更 サブスクリプションのコピー サブスクリプションの削除 アップデートマネージャの設定
ポリシー設定 - Web コントロール	Web コントロール ポリシーの作成 Web コントロール ポリシーのコピー Web コントロール ポリシーの名前の変更 Web コントロール ポリシーの編集 Web コントロール ポリシーの設定をデフォルトに戻す Web コントロール ポリシーの削除
ポリシー設定 - エクスプロイト対策	エクスプロイト対策ポリシーの作成 エクスプロイト対策ポリシーのコピー エクスプロイト対策ポリシーの名前の変更 エクスプロイト対策ポリシーの編集 エクスプロイト防止の除外の追加 エクスプロイト防止の除外の削除 エクスプロイト対策ポリシーのリセット エクスプロイト対策ポリシーの削除

権限	タスク
修復 - クリーンアップ	検出されたアイテムのクリーンアップ 警告の消去 エラーの消去
修復 - アップデートと検索	コンピュータの即時アップデート コンピュータのフル検索の実行 コンピュータへのグループポリシーの強制適用 アップデートマネージャへの環境設定の適用 アップデートマネージャで今すぐアップデート
レポート環境設定	レポートの作成、編集、または削除
ロールベースの管理	ロールの作成 ロール名の変更 ロールの削除 ロールの権限の変更 ロールへのユーザーやグループの追加 ロールからのユーザーやグループの削除 サブ管理サイトの管理: サブ管理サイトの作成、サブ管理サイト名の変更、サブ管理サイトの削除、サブ管理サイトのルートグループの追加、サブ管理サイトのルートグループの削除、サブ管理サイトへのユーザーやグループの追加、サブ管理サイトからのユーザーやグループの削除
システム環境設定	SMTP サーバーの設定の変更、SMTP サーバーの設定のテスト、メール警告の受信者の変更 ダッシュボードの警報・緊急レベルの設定 レポートの設定: データベースの警告の初期化設定、レポートに表示する会社名の設定 ソフォスへのレポート送信の設定: ソフォスへのレポート送信の有効/無効の切り替え、ユーザー名の変更、連絡先メールアドレスの変更 固定バージョンのソフトウェアパッケージの使用設定
Web のイベント	Web のイベントビューアの表示 「コンピュータの詳細」ダイアログボックスへの Web のイベントの表示

4.1.13 新しい Enterprise Console ユーザーを追加する

Sophos Full Administrators グループに所属するユーザーには、Enterprise Console に対するフルアクセス権限が付与されています。

他のユーザーに Enterprise Console の使用を許可できます。Enterprise Console を開くことができるユーザーの条件は次のとおりです。

- Sophos Console Administrators グループのメンバーである。
- 少なくとも 1つの Enterprise Console ロールに追加されている。
- 少なくとも 1つの Enterprise Console サブ管理サイトに追加されている。

Sophos Console Administrators グループにユーザーを追加する場合は、Windows の機能を使ってください。

Enterprise Console のロールやサブ管理サイトにユーザを追加するには、「**ツール**」メニューで、「**ロールとサブ管理サイトの管理**」をクリックします。ロールとサブ管理サイトの詳細はロールとサブ管理サイトを管理する (p. 14)を参照してください。

リモートの管理コンソールや、追加の Enterprise Console を使用できるユーザーの条件は次のとおりです。

- Enterprise Console の管理サーバーがインストールされているサーバー上の Sophos Console Administrators グループのメンバーである。
- Enterprise Console の管理サーバーがインストールされているサーバー上の Distributed COM Users グループのメンバーである。(Distributed COM Users グループは、「Active Directory ユーザーとコンピュータ」ツールのビルトインコンテナにあります。)
- 少なくとも 1つの Enterprise Console ロールに追加されている。
- 少なくとも 1つの Enterprise Console サブ管理サイトに追加されている。

4.2 グループを作成、使用する

コンピュータの保護・管理を行うためには、まず、グループを作成して、コンピュータを配置する必要があります。

4.2.1 グループを使用する理由

コンピュータのグループを作成する利点は次のとおりです。

- グループごとに、個別のアップデート元やスケジュールを設定してアップデートできる。
- グループごとに、個別のウイルス対策および HIPS、アプリケーション コントロール、ファイアウォール、および他のポリシーを適用できる。
- コンピュータの管理がしやすくなる。

ヒント
グループ内にさらにグループを作成し、各グループやサブグループごとに一連のポリシーを適用することができます。

4.2.2 グループとは？

グループ

は、複数のコンピュータが含まれるフォルダです。

グループは手動で作成するか、または Active Directory のコンテナを (コンピュータの有無に関わらず) インポートすることができます。インポートしたコンテナを Enterprise Console のコンピュータのグループとして使います。また、新規コンピュータやコンテナ、および Active Directory における他の変更内容が Enterprise Console に自動的にコピーされるよう、Active Directory との同期を設定することもできます。

各グループに対して、アップデート、ウイルス対策および HIPS 機能、ファイアウォールなどを設定できます。グループ内の各コンピュータは、通常、すべて同じ設定内容 (「ポリシー」と呼びます) を使用する必要があります。

1つのグループ内に複数のサブグループを作成することもできます。

4.2.3 「グループ外のコンピュータ」フォルダとは？

Enterprise Console の「**グループ外のコンピュータ**」フォルダには、グループに配置する前のコンピュータが入っています。

次の事柄を実行することはできません。

- 「**グループ外のコンピュータ**」フォルダにポリシーを適用する。
- 「**グループ外のコンピュータ**」フォルダにサブフォルダを作成する。
- 「**グループ外のコンピュータ**」フォルダを移動・削除する。

4.2.4 グループを作成する

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

コンピュータの新規グループを作成する方法は次のとおりです。

1. 「**エンドポイント**」ビューの「**グループ**」ペイン (コンソール画面の左側) で、グループを作成する場所を選択します。

   トップレベルのグループを新たに作成するには、ツリー最上部のコンピュータ名をクリックします。サブグループを作成するには、既存のグループをクリックします。
2. ツールバーで、「**グループの作成**」アイコンをクリックします。
   「新規グループ」がリストに追加され、グループ名がハイライト表示されます。
3. グループ名を入力します。

アップデート、ウイルス対策および HIPS、アプリケーション コントロール、ファイアウォール、パッチ、データコントロール、デバイスコントロール、タンパー プロテクション、および Web コントロール ポリシーは、新規グループに自動的に適用されます。これらのポリシーを編集したり、別のポリシーを適用することもできます。詳細は、ポリシーを編集する (p. 31)またはグループにポリシーを適用する (p. 31)を参照してください。

注
新規グループがサブグループの場合、初期設定内容は親グループと同じです。

4.2.5 グループにコンピュータを追加する

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. グループに追加するコンピュータを選択します。たとえば、「**グループ外のコンピュータ**」フォルダをクリックし、表示されるコンピュータを選択します。
2. 新規グループに選択したコンピュータをドラッグ & ドロップします。

   保護されていないコンピュータを、「**グループ外のコンピュータ**」フォルダから自動アップデートが設定されているグループに移動した場合は、ウィザードが開始するので、指示に従ってコンピュータを保護してください。

   グループ内のコンピュータを別のグループに移動した場合、移動したコンピュータには、移動先グループ内の他のコンピュータと同じポリシーが適用されます。

4.2.6 グループからコンピュータを削除する

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ネットワーク上に存在しないコンピュータなど、コンピュータをグループから削除することができます。

重要
ネットワーク上のコンピュータを削除すると、削除されたコンピュータはコンソール画面より表示、または管理されなくなります。

旧バージョンの Enterprise Console からアップグレードした場合で、フルディスク暗号化管理機能が搭載されていた古いバージョンの Enterprise Console で暗号化したコンピュータがあるときは、これらのコンピュータをコンソールから削除しないでください。削除すると、暗号化の復旧ができなくなる可能性があります。

コンピュータを削除する方法は次のとおりです。

1. 削除するコンピュータを選択します。
2. 右クリックして、「**削除**」を選択します。

削除したコンピュータを再表示するには、ツールバーにある「**コンピュータの検出**」アイコンをクリックします。これらのコンピュータは再起動すると、管理対象コンピュータとして表示されます。

4.2.7 グループを切り取り、貼り付ける

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 切り取り、貼り付けるグループを選択します。「**編集**」メニューの「**切り取り**」をクリックします。
2. 貼り付け先のグループを選択します。「**編集**」メニューの「**貼り付け**」をクリックします。

4.2.8 グループを削除する

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

グループ削除後、グループ内のコンピュータは、「**グループ外のコンピュータ**」フォルダに配置されます。

1. 削除するグループを選択します。
2. 右クリックして、「**削除**」を選択します。メッセージが表示されたら、グループを削除することを確認し、サブグループが存在する場合はそれも削除することを確認します。

4.2.9 グループ名の変更

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 名前を変更するグループを選択します。
2. 右クリックして、「**名前の変更**」を選択します。

4.2.10 グループに適用されているポリシーを確認する

グループに適用されているポリシーを表示する方法は次のとおりです。

- 「**グループ**」ペインで、グループ名を右クリックします。「**グループポリシーの詳細の表示/編集**」を選択します。

  グループの詳細ダイアログボックスに、現在使用されているポリシーが表示されます。

4.3 ポリシーを作成、使用する

ポリシーは、グループ内のすべてのコンピュータに適用される設定の集まりです。

Enterprise Console をインストールすると、基本的なレベルのセキュリティを提供する「デフォルト」ポリシーが作成されます。デフォルトポリシーは、新たに作成するグループすべてに適用されます。デフォルトのポリシーを編集したり、または新しいポリシーを作成できます。

注
ライセンスの種類により利用できない機能もあります。

各種類につき、複数のポリシーを作成できます。

複数のグループに同じポリシーを適用することができます。

4.3.1 利用可能なポリシー

注
ライセンスの種類により利用できない機能もあります。

- **アップデート**ポリシー: 新しいセキュリティソフトでコンピュータがアップデートされる方法を指定します。
- **ウイルス対策および HIPS** ポリシー: セキュリティソフトがウイルス、トロイの木馬、ワーム、スパイウェア、アドウェア、および不要と思われるアプリケーションを検索し、疑わしい動作や

ファイルを検知・検出する方法を指定します。また、コンピュータをクリーンアップする方法も指定します。

- **アプリケーション コントロール**ポリシー: コンピュータでブロック・許可するアプリケーションを指定します。
- **ファイアウォール**ポリシー: ファイアウォールがコンピュータを保護する方法を指定します。
- **データコントロール**ポリシー: ファイルの内容、名前、または種類に基づいて、ファイルの転送を監視・制限するルールを指定します。
- **デバイスコントロール**ポリシー: クライアントマシンでの使用を認証しないストレージデバイスやネットワーク機器を指定します。
- **パッチ**ポリシー: パッチ評価の有効化/無効化、および未適用のパッチがあるかを評価する頻度を設定します。
- **タンパー プロテクション** ポリシー: ソフォスのセキュリティソフトの再設定、無効化、アンインストールを認証済みエンドポイントユーザーに許可するパスワードを指定します。
- **Web コントロール** ポリシー: ユーザーにアクセスを許可する Web サイトを指定します。「ブロック」または「警告」に指定されている Web サイトにユーザーがアクセスするとメッセージが表示されます。
- **エクスプロイト対策**ポリシー: エクスプロイトから防御するアプリケーションや機能、プロセスを指定します。たとえば、ランサムウェアから文書ファイルを保護したり (CryptoGuard)、Web ブラウザの重要な機能を保護したり (セーフブラウジング) することができます。

4.3.2 デフォルトポリシー

Enterprise Console をインストールすると、「デフォルト」というポリシーが作成されます。

注
ライセンスの種類により利用できない機能もあります。

アップデートポリシー

Enterprise Console を新規にインストールすると、デフォルトのアップデートポリシーは次のように設定されます。

- デフォルトのアップデート元から 10分ごとにコンピュータを自動アップデートする。デフォルトのアップデート元は、UNC 共有の ¥¥<コンピュータ名>¥SophosUpdate です。ここで、<コンピュータ名> は、アップデートマネージャをインストールしたコンピュータの名前です。

ウイルス対策および HIPS ポリシー

Enterprise Console を新規にインストールすると、デフォルトのウイルス対策および HIPS ポリシーは次のように設定されます。

- ウイルス、トロイの木馬、ワーム、スパイウェア、アドウェア、および不要と思われるアプリケーション (疑わしいファイルは除く) のオンアクセス検索を実施する。
- バッファオーバーフローや、システム上で実行されているプログラムの悪意のある、または疑わしい動作、および悪質なネットワークトラフィックを検知する。
- マルウェア感染サイトへのアクセスをブロックする。
- インターネットからダウンロードしたコンテンツを検索する。

- 問題のあるコンピュータのデスクトップでセキュリティ警告を表示し、イベントログに追加する。

Enterprise Console を新規にインストールした場合のウイルス対策および HIPS ポリシーのデフォルト設定については、サポートデータベースの文章 27267 を参照してください。

アプリケーション コントロール ポリシー

デフォルトで、すべてのアプリケーションおよびアプリケーションのタイプは許可されています。ネットワークでの使用制御が必要と思われるアプリケーションのオンアクセス検索は、デフォルトで無効に設定されています。

ファイアウォールポリシー

デフォルトで、Sophos Client Firewall は有効に設定され、必須のトラフィック以外はすべてブロックされます。ネットワーク全体でファイアウォールを使用する前に、必要なアプリケーションの使用を許可するようファイアウォールを設定してください。詳細は、基本的なファイアウォールポリシーを設定する (p. 113)を参照してください。

デフォルトのファイアウォール設定について、詳細はサポートデータベースの文章 57757 を参照してください。

データコントロール ポリシー

デフォルトで、データコントロールは無効になっています。インターネットを経由したファイル転送や、ストレージデバイスへのファイル転送を監視・制限するルールも指定されていません。

デバイス コントロール ポリシー

デフォルトで、デバイス コントロールは無効になっています。すべてのデバイスが許可されています。

パッチポリシー

デフォルトでパッチ評価は無効になっています。新しいパッチポリシーについては評価が有効になります。パッチ評価を有効にすると、コンピュータにインストールされていないパッチの有無が毎日 (チェック頻度を変更していない場合) チェックされます。

タンパー プロテクション ポリシー

デフォルトで、タンパー プロテクションは無効になっており、認証済みエンドポイントユーザーに、ソフォスのセキュリティソフトの再設定、無効化、アンインストールを許可するパスワードは指定されていません。

Web コントロール ポリシー

デフォルトで、Web コントロールは無効になっているため、Enterprise Console の Web Protection 機能で制限されていない限り、すべての Web サイトにアクセスできます。詳細は、Web Protection (p. 101)を参照してください。

エクスプロイト対策ポリシー

デフォルトで、エクスプロイト対策は有効になっています。詳細は、エクスプロイト対策ポリシー (p. 185)を参照してください。

4.3.3 デフォルト以外のポリシーの必要性について

Enterprise Console をインストールすると、「デフォルト」というポリシーが作成されます。デフォルトポリシーは、新たに作成するグループすべてに適用されます。

デフォルトポリシーは、基本的なレベルのセキュリティを提供します。ネットワーク アクセス コントロールやアプリケーション コントロールなどの機能を使用するには、新たにポリシーを作成するか、デフォルトポリシーの設定内容を変更する必要があります。

注
デフォルトのポリシーを変更すると、今後新しく作成するポリシーすべてに変更内容が反映されます。

注
ロールベースの管理を利用している場合、ポリシーを作成または設定するには、該当する「**ポリシー設定**」権限が必要です。たとえば、ウイルス対策および HIPS ポリシーを作成または設定するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

アップデートポリシー

デフォルトのアップデートポリシーを適用すると、エンドポイントは、デフォルトのソフトウェア配布元 UNC 共有に、「Recommended」サブスクリプションのアップデートがあるかどうかを 10 分ごとに確認するようになります。サブスクリプション、アップデート元、およびその他の設定を変更するには、アップデートポリシーの設定を変更してください。詳細はアップデートポリシーを設定する (p. 68)を参照してください。

ウイルス対策および HIPS

デフォルトのウイルス対策および HIPS ポリシーは、ウイルスやその他のマルウェアからコンピュータを保護します。他の不要と思われる/疑わしいアプリケーションや動作を検出・検知するには、新たにポリシーを作成するか、デフォルトポリシーを変更してください。詳細は、ウイルス対策および HIPS ポリシー (p. 80)を参照してください。

アプリケーション コントロール

未認証のアプリケーションを定義したり、ブロックするには、アプリケーション コントロール ポリシーを設定してください。詳細は、アプリケーション コントロール ポリシー (p. 146)を参照してください。

ファイアウォールポリシー

正規アプリケーションのネットワークアクセスを許可するには、ファイアウォールポリシーを設定してください。詳細は、ファイアウォール ポリシー (p. 113)を参照してください。

データコントロール

デフォルトで、データコントロールは無効になっています。データ漏えいを防止するには、データコントロール ポリシーを設定してください。詳細は、データコントロール ポリシー (p. 149)を参照してください。

デバイスコントロール

デフォルトで、デバイスコントロールは無効になっています。使用を許可するハードウェアデバイスを制限するには、デバイスコントロール ポリシーを設定してください。詳細は、デバイスコントロール ポリシー (p. 164)を参照してください。

パッチ

デフォルトでパッチ評価は無効になっています。新しいパッチポリシーについては評価が有効になります。パッチ評価を有効にすると、コンピュータにインストールされていないパッチの有無が毎日 (チェック頻度を変更していない場合) チェックされます。パッチ評価を有効/無効に切り替えたり、評価の頻度を変更するには、パッチポリシーを設定してください。詳細は、パッチ ポリシー (p. 175)を参照してください。

タンパー プロテクション

デフォルトで、タンパー プロテクションは無効になっています。タンパー プロテクションを有効にするには、タンパー プロテクション ポリシーを設定してください。詳細は、タンパー プロテクション ポリシー (p. 172)を参照してください。

Web コントロール

デフォルトで、Web コントロールは無効になっています。Web コントロールを有効にして、Web コントロールポリシーを設定するには、Web コントロール ポリシー (p. 177)を参照してください。

エクスプロイト対策

デフォルトで、エクスプロイト対策は有効になっています。エクスプロイト対策ポリシーの設定方法については、エクスプロイト対策ポリシー (p. 185)を参照してください。

4.3.4 ポリシーを作成する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、該当する「**ポリシー設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ポリシーの作成方法は次のとおりです。

1. 「**エンドポイント**」ビューの「**ポリシー**」ペインで、「アップデート」ポリシーなど、作成するポリシーの種類を右クリックし、「**ポリシーの作成**」を選択します。
   「新規ポリシー」がリストに追加され、ポリシー名がハイライト表示されます。
2. 新しいポリシーの名前を入力します。
3. 新しいポリシーをダブルクリックします。必要に応じて内容を設定します。

   各設定の選択方法について詳細は、ポリシー別の設定に関するセクションを参照してください。

これで、グループに適用できるポリシーが作成されました。

4.3.5 グループにポリシーを適用する

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**ポリシー**」ペインで、ポリシー名をハイライト表示します。
2. 選択したポリシーをクリックして、適用するグループの上にドラッグ & ドロップします。確認メッセージが表示されたら、続行することを指定します。

注
または、各グループを右クリックして、「**グループポリシーの詳細の表示/編集**」を選択します。表示されるドロップダウンメニューから、そのグループに対するポリシーを選択できます。

4.3.6 ポリシーを編集する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、各ポリシーに対応する「**ポリシー設定**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

グループやグループ内のコンピュータに対するポリシーを編集する方法は次のとおりです。

1. 「**ポリシー**」ペインで、編集するポリシーをダブルクリックします。
2. ポリシーの内容を編集します。

ポリシーの種類別の設定方法については、各セクションを参照してください。

4.3.7 ポリシー名を変更する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、各ポリシーに対応する「**ポリシー設定**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーの名前だけ変更できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

注
「デフォルト」ポリシーの名前を変更することはできません。

ポリシー名の変更方法は次のとおりです。

1. 「**ポリシー**」ペインで、名前を変更するポリシーを選択します。
2. 右クリックして、「**ポリシー名の変更**」を選択します。

4.3.8 ポリシーの削除

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、各ポリシーに対応する「**ポリシー設定**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ削除できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

注
「デフォルト」ポリシーを削除することはできません。

ポリシーを削除する方法は次のとおりです。

1. 「**ポリシー**」ペインで、削除するポリシーを右クリックし、「**ポリシーの削除**」を選択します。
2. 削除したポリシーを使用していたグループは、デフォルトポリシーを使用するようになります。

4.3.9 ポリシーが適用されているグループを表示する

各ポリシーが適用されているグループを表示する方法は次のとおりです。

- 「**ポリシー**」ペインで、ポリシーを右クリックし、「**ポリシー別グループの表示**」を選択します。

  選択したポリシーが適用されているグループが表示されます。

4.3.10 コンピュータがグループ固有のポリシーを使用しているか確認する

グループ内のコンピュータすべてがポリシーに準拠しているかを確認することができます。

1. 確認するグループを選択します。
2. 「**エンドポイント**」ビューのコンピュータのリストで、「**ステータス**」タブを開き、「**ポリシーコンプライアンス**」カラムの表示を確認します。
   - 「ポリシーと一致」と表示されている場合は、コンピュータがグループに適用されているポリシーに準拠していることを意味します。
   - 黄色い警告アイコン付きで「ポリシーと異なる」と表示されている場合は、グループ内の他のコンピュータと異なるポリシー (複数の場合もあります) が適用されていることを意味します。

   コンピュータ上のセキュリティ機能のステータスや、コンピュータに適用されているポリシーのステータスの詳細は、「**エンドポイント**」ビューの各タブをご覧ください (「**ウイルス対策の詳細**」タブなど)。

所属するグループのポリシーをコンピュータに適用する場合は、コンピュータにグループ固有のポリシーを適用する (p. 33)を参照してください。

4.3.11 コンピュータにグループ固有のポリシーを適用する

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**修復 - アップデートと検索**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

グループに適用されているポリシーに準拠していないコンピュータを見つけた場合、そのコンピュータにグループ固有のポリシーを適用できます。

1. グループ固有のポリシーに準拠していないコンピュータを選択します。
2. 右クリックして、「**ポリシーの適用**」を選択します。次に、「**グループのウイルス対策およびHIPS ポリシー**」など、適切な種類のポリシーを選択します。

4.4 ネットワーク上のコンピュータを検出する

Enterprise Console でコンピュータを管理するには、まず、Enterprise Console に追加する必要があります。「コンピュータの検出」機能のオプションを使用して、ネットワーク上のコンピュータを検出し、Enterprise Console に追加することができます。次のオプションがあります。

- Active Directory からコンテナやコンピュータをインポートする (p. 33)
- Active Directory を使用してコンピュータを検出する (p. 34)
- ネットワーク上のコンピュータを検出する (p. 35)
- IP アドレス範囲を指定してコンピュータを検出する (p. 35)
- ファイルからコンピュータ名をインポートする (p. 36)

ロールベースの管理を利用している場合、各コンピュータをコンソールに追加するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

4.4.1 Active Directory からコンテナやコンピュータをインポートする

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Active Directory からグループをインポートすると、Active Directory のコンテナ構成が取得され、そのコピーがコンピュータのグループの階層として Enterprise Console に保存されます。グループの階層構造だけをインポートすることも、グループとコンピュータをインポートすることもできます。グループとコンピュータをインポートした場合は、Active Directory で検出されるコンピュータは、「**グループ外のコンピュータ**」フォルダではなく、所属する各グループ内に配置されます。

この製品で作成および管理する「通常」のグループと、Active Directory からインポートしたグループの両方を持つことができます。また、インポートしたグループを Active Directory と同期することもできます。

Active Directory からグループをインポートする方法は次のとおりです。

1. ツールバーの「**コンピュータの検出**」アイコンをクリックします。
2. 「**コンピュータの検出**」ダイアログボックスの「**Active Directory のインポート**」ペインで、「**インポート**」を選択し、「**OK**」をクリックします。

   あるいは、Active Directory コンテナをインポートするグループを選択し、右クリックして、「**Active Directory のインポート**」を選択します。

   「**Active Directory のインポート ウィザード**」が開始します。
3. ウィザードの指示に従います。インポートするアイテムを選択するページで、インポート内容に従い、「**コンピュータとコンテナ**」または「**コンテナのみ**」を選択します。

Active Directory からコンテナをインポートした後は、そのグループにポリシーを適用します。詳細は、利用可能なポリシー (p. 26)を参照してください。

グループにポリシーを適用した後は、必要に応じて、グループと Active Directory の同期をとることができます。手順については、Active Directory と同期する (p. 36)を参照してください。

4.4.2 Active Directory を使用してコンピュータを検出する

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Active Directory を使ってネットワーク上のコンピュータを検出し、「**グループ外のコンピュータ**」フォルダに追加することができます。

1. ツールバーの「**コンピュータの検出**」アイコンをクリックします。
2. 「**コンピュータの検出**」ダイアログボックスで、「**Active Directory の検出**」を選択し、「**OK**」をクリックします。
3. ユーザー名とパスワードを入力するようメッセージが表示されます。アカウント情報なしでアクセスできないコンピュータ (例: Windows XP サービスパック 2) の場合は、この作業を行う必要があります。

   ドメイン管理者アカウント、または対象の Windows XP コンピュータに対してフル管理者権限を持つアカウントを使用してください。

   ドメインアカウントを使用している場合は、必ず、ドメイン名¥ユーザー名 という形式でユーザー名を入力してください。
4. 「**コンピュータの検出**」ダイアログボックスで、検索するドメインを選択します。「**OK**」をクリックします。
5. 「**グループ外のコンピュータ**」フォルダをクリックして、検出されたコンピュータを表示します。

管理を開始するには、これらのコンピュータを選択し、グループにドラッグ & ドロップしてください。

4.4.3 ネットワーク上のコンピュータを検出する

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Windows ドメイン、およびワークグループで検出されたコンピュータを、「**グループ外のコンピュータ**」フォルダに追加する方法は次のとおりです。

1. ツールバーの「**コンピュータの検出**」アイコンをクリックします。
2. 「**コンピュータの検出**」ダイアログボックスで、「**ネットワークの検出**」を選択し、「**OK**」をクリックします。
3. 「**アカウント情報**」ダイアログボックスで、コンピュータの情報を取得する十分な権限のあるアカウントのユーザー名とパスワードを入力します。

   ドメイン管理者アカウント、または対象のコンピュータに対してフル管理者権限を持つアカウントを使用してください。ドメインアカウントを使用している場合は、必ず、ドメイン名¥ユーザー名 という形式でユーザー名を入力してください。

   対象のコンピュータにアカウント情報なしでアクセスできる場合は、このステップは必要ありません。
4. 「**コンピュータの検出**」ダイアログボックスで、検索するドメインやワークグループを選択します。「**OK**」をクリックします。
5. 「**グループ外のコンピュータ**」フォルダをクリックして、検出されたコンピュータを表示します。

管理を開始するには、これらのコンピュータを選択し、グループにドラッグ & ドロップしてください。

4.4.4 IP アドレス範囲を指定してコンピュータを検出する

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

IP アドレスの範囲を指定してネットワーク上のコンピュータを検出し、「**グループ外のコンピュータ**」フォルダに追加することができます。

注
IPv6 アドレスを使用することはできません。

1. ツールバーの「**コンピュータの検出**」アイコンをクリックします。
2. 「**コンピュータの検出**」ダイアログボックスで、「**IP アドレス範囲を指定して検出**」を選択し、「**OK**」をクリックします。
3. 「**アカウント情報**」ダイアログボックスで、ユーザー名とパスワードを入力するようメッセージが表示されます。アカウント情報なしでアクセスできないコンピュータ (例: Windows XP サービスパック 2) の場合は、この作業を行う必要があります。

   ドメイン管理者アカウント、または対象の Windows XP コンピュータに対してフル管理者権限を持つアカウントを使用してください。

   ドメインアカウントを使用している場合は、必ず、ドメイン名¥ユーザー名 という形式でユーザー名を入力してください。

   「**SNMP**」ペインで SNMP コミュニティ名を入力できます。

4. 「**コンピュータの検出**」ダイアログボックスで、「**開始 IP アドレス**」と「**終了 IP アドレス**」を入力します。「**OK**」をクリックします。
5. 「**グループ外のコンピュータ**」フォルダをクリックして、検出されたコンピュータを表示します。

管理を開始するには、これらのコンピュータを選択し、グループにドラッグ & ドロップしてください。

4.4.5 ファイルからコンピュータ名をインポートする

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Enterprise Console で、ファイルからコンピュータ名をインポートし、お使いのコンピュータを一覧表示できます。次のようなエントリを含むファイルを作成することができます。

```
[グループ名1]
 ドメイン名1|Windows7|コンピュータ名1
 ドメイン名1|Windows2008ServerR2|コンピュータ名2
```

注
コンピュータを配置するグループの指定は任意です。グループ名として [] (カッコの間に空白文字は入れません) を入力すると、コンピュータは、「**グループ外のコンピュータ**」フォルダに配置されます。

有効な OS 名:
WindowsXP、Windows2003、WindowsVista、Windows7、WindowsServer2008、Windows2008ServerR2、

ドメイン名と OS 名は共に任意です。エントリの一例は次のとおりです。

```
[グループ名1]
 コンピュータ名1
```

コンピュータ名をインポートする方法は次のとおりです。

1. 「**ファイル**」メニューの「**ファイルからコンピュータ名をインポート**」をクリックします。
2. 参照ウィンドウでファイルを選択します。
3. 「**グループ外のコンピュータ**」フォルダをクリックして、検出されたコンピュータを表示します。
4. 管理を開始するには、これらのコンピュータを選択し、グループにドラッグ & ドロップしてください。

4.5 Active Directory と同期する

ここでは Active Directory との同期の概要について説明します。

Active Directory の同期とは？

Active Directory の同期で、Enterprise Console グループと Active Directory コンテナを同期することができます。Active Directory で検出される新しいコンピュータやコンテナは、Enterprise

Console に自動的にコピーされます。また、検出された Windows のクライアントマシンの自動保護を選択することもできます。これにより、コンピュータが保護されるまでの無防備な時間が短縮され、また、保護の作業負担が軽減されます。

注
Mac OS、Linux、または UNIX が稼動しているコンピュータは自動保護されません。このようなコンピュータは手動で保護する必要があります。

同期の設定が完了したら、以後、同期中にコンピュータやコンテナが新しく検出された際に、特定の宛先にメール警告を送信するように設定できます。同期した Enterprise Console のグループ内のコンピュータを自動保護する場合は、自動保護に失敗した場合に警告を送信するように設定することもできます。

Active Directory の同期方法

Enterprise Console では、この製品で作成・管理する同期を行わない「通常」のグループと、Active Directory と同期するグループの両方を持つことができます。

同期を設定する際に、Active Directory コンテナと常に同期する Enterprise Console グループ (同期ポイント) を選択、または作成します。Active Directory コンテナに含まれるすべてのコンピュータやサブグループは、Enterprise Console にコピーされ、常に Active Directory と同期されます。

注
同期ポイントの詳細については、同期ポイントとは？ (p. 38)を参照してください。同期したグループの詳細については、同期したグループとは？ (p. 38)を参照してください。

Active Directory との同期の設定が完了すると、同期設定した部分の Enterprise Console のグループ構成が同期をとる Active Directory のコンテナ構成と全く同じになります。変更は次のように反映されます。

- Active Directory コンテナに新規コンピュータが追加されると、Enterprise Console にも表示されます。
- Active Directory からコンピュータを削除したり、同期していないコンテナに移動した場合、それらのコンピュータは、Enterprise Console では「**グループ外のコンピュータ**」フォルダに移動されます。

  注
  「**グループ外のコンピュータ**」フォルダに移動されたコンピュータには、新しいポリシーが適用されなくなります。

- 同期するコンテナ間でコンピュータが移動されると、Enterprise Console でもグループ間でコンピュータが移動されます。
- はじめて同期する際に、Enterprise Console のグループ内に既にコンピュータが存在する場合は、同期する Active Directory の構成と一致するグループに移動されます。
- 新しいグループに移動したコンピュータのポリシーが移動先のポリシーと異なる場合は、当該のコンピュータに新しいポリシーが送信されます。

デフォルトで、同期は 1時間ごとに行われます。同期の間隔は、必要に応じて変更できます。

同期の設定にあたって

Active Directory と同期するグループや、設定する同期ポイントの数は自由に決めることができますが、作成されるグループのサイズが管理可能な大きさであるかを考慮してください。無理なくコンピュータにソフトウェアをインストールし、検索・クリーンアップできるようにしてください。これは特に、初回のインストールにおいて重要です。

注
Active Directory の構成が複雑な場合で、ドメインローカルグループやネストされた Active Directory グループを同期するときは、この機能の有効化の詳細について、サポートデータベースの文章 122529 を参照してください。

推奨する方法は次のとおりです。

1. 「**Active Directory のインポート**」機能を使用して、グループ構成 (コンピュータなし) をインポートします。手順については、Active Directory からコンテナやコンピュータをインポートする (p. 33)を参照してください。
2. インポートしたグループ構成を確認して、同期ポイントを選択します。
3. グループポリシーを設定し、グループおよびサブグループに適用します。手順については、ポリシーを作成する (p. 31)、およびグループにポリシーを適用する (p. 31)を参照してください。
4. 選択した同期ポイントを 1つずつ Active Directory と同期します。手順については、Active Directory と同期する (p. 39)を参照してください。

4.5.1 同期ポイントとは？

「同期ポイント」とは、Active Directory にあるコンテナ (またはサブツリー) を指定する Enterprise Console のグループです。1つの同期ポイントには、Active Directory からインポートされた同期したグループが含まれることもあります。

「**グループ**」ペインで、同期ポイントは次のように表示されます。

同期ポイントは、移動、名前を変更、または削除できます。また、自動保護の設定など、同期ポイントのポリシーや同期の設定内容を変更することができます。

同期ポイントでサブグループを作成、または削除したり、他のグループを同期ポイントに移動することはできません。同期ポイントへコンピュータを移動したり、同期ポイントからコンピュータを移動することはできません。

4.5.2 同期したグループとは？

「同期したグループ」とは、Active Directory からインポートした同期ポイントのサブグループです。

「**グループ**」ペインで、同期したグループは次のように表示されます。

同期したグループに適用されているポリシーを変更することができます。

グループポリシー以外の同期したグループの設定内容は、変更できません。同期したグループを、名前の変更、移動、または削除することはできません。同期したグループへコンピュータを移動したり、同期したグループからコンピュータを移動することはできません。グループ内にサブグループを作成したり、またはグループ内のサブグループを削除することはできません。グループの同期設定を変更することはできません。

4.5.3 Active Directory と同期する

ここでの手順を実行する前に次の項目を確認してください。

- ロールベースの管理を利用する場合、「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。
- 同期しているグループ内のコンピュータを自動で保護する場合は、セキュリティソフトをインストールするための準備をする (p. 44)の説明に従い、コンピュータの準備が済んでいることを確認してください。
- Active Directory の構成が複雑な場合で、ドメインローカルグループやネストされた Active Directory グループを同期するときは、サポートデータベースの文章 122529 の説明に従ってこの機能を有効化してください。

Active Directory と同期する方法は次のとおりです。

1. 同期ポイントとなるグループを選択して右クリックし、「**Active Directory の同期**」を選択します。
   「**Active Directory の同期 ウィザード**」が開始します。
2. ウィザードの「**概要**」ページで、「**次へ**」をクリックします。
3. 「**Enterprise Console グループの選択**」ページで、Active Directory と常に同期する Enterprise Console のグループ (同期ポイント) を選択、または作成します。「**次へ**」をクリックします。
4. 「**Active Directory コンテナの選択**」ページで、グループと同期する Active Directory コンテナを選択します。たとえば、次のようにコンテナ名を入力します。LDAP://CN=Computers,DC=domain_name,DC=local。または、「**参照**」をクリックして Active Directory にあるコンテナを参照します。「**次へ**」をクリックします。

   重要
   同期している複数の Active Directory のコンテナに所属するコンピュータがある場合は、そのコンピュータと Enterprise Console との間で常にメッセージが送受信され、問題が発生します。Enterprise Console のリスト内で、コンピュータが重複しないようにしてください。

5. Windows のクライアントマシンを自動保護する場合は、「**コンピュータの自動保護**」ページで、「**ソフォスのセキュリティソフトを自動インストールする**」チェックボックスを選択します。そして、インストールするソフトウェアを選択します。

   注
   ソフトウェアに対するシステム要件の詳細は、ソフォス Web サイトの「システム要件」(http://www.sophos.com/ja-jp/products/all-system-requirements.aspx) を参照してください。

   - **Firewall** をコンピュータにインストールする前に、必要なトラフィック、アプリケーション、およびプロセスを許可するようにファイアウォールを構成していることを確認します。デフォルトで、ファイアウォールは有効に設定されるため、必須のトラフィック以外はすべてブロックされます。詳細は、ファイアウォール ポリシー (p. 113)を参照してください。

- 他社製セキュリティ対策ソフトを自動削除する場合は、「**Third-Party Security Software Detection**」を選択したままにしておいてください。他社製のアップデートツールをアンインストールする必要がある場合は、他社製セキュリティ対策ソフトを削除する (p. 44)を参照してください。

同期中に検出されるすべての Windows のクライアントマシンは自動で保護され、所属する各グループのポリシーが適用されます。

重要
Mac OS、Linux、または UNIX が稼動しているコンピュータは自動保護できません。これらのコンピュータは手動で保護する必要があります。詳細は「Sophos Enterprise Console アドバンス スタートアップガイド」を参照してください。

注
コンピュータの自動保護は、後で有効/無効に切り替えることができます。設定場所は、「**同期のプロパティ**」ダイアログボックスです。手順については、同期のプロパティを表示・編集する (p. 41)を参照してください。

「**次へ**」をクリックします。

6. コンピュータの自動保護を選択する場合は、「**Active Directory アカウント情報の入力**」ページで、コンピュータにソフトウェアをインストールする際に使用する管理者アカウントの詳細を入力します。「**次へ**」をクリックします。
7. 「**同期の頻度の選択**」ページで、Enterprise Console グループと Active Directory コンテナを同期する頻度を選択します。デフォルトは 60分です。

注
同期の頻度は、後で変更することができます。設定場所は、「**同期のプロパティ**」ダイアログボックスです。手順については、同期のプロパティを表示・編集する (p. 41)を参照してください。

8. 「**選択内容の確認**」ページで、詳細を確認後、「**次へ**」をクリックして続行します。
9. ウィザードの最後のページに、同期されたグループやコンピュータの詳細が表示されます。

また、同期中にコンピュータやグループが新しく検出された際に、特定の宛先にメール警告を送信するように設定できます。同期したグループ内のコンピュータを自動保護する場合は、自動保護に失敗した場合に警告を送信するように設定することもできます。「**完了**」をクリックした後に、「**メール警告の環境設定**」ダイアログボックスを開くには、ウィザードの最後のページにあるチェックボックスを選択します。手順については、Active Directory との同期のメール警告を設定する (p. 197)を参照してください。

ウィザードを終了するには、「**完了**」をクリックします。

4.5.4 同期を利用してコンピュータを自動的に保護する

ここでの手順を実行する前に次の項目を確認してください。

- ロールベースの管理を利用する場合、「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。
- セキュリティソフトをインストールするための準備をする (p. 44)の説明に従い、コンピュータにセキュリティソフトを自動でインストールするための準備を行ったことを確認してください。

Windows クライアントマシンは、Active Directory との同期中に検出されると自動的に保護されます。

重要
Mac OS、Linux、または UNIX が稼動しているコンピュータは自動的に保護されません。これらのコンピュータは手動で保護する必要があります。詳細は「Sophos Enterprise Console アドバンス スタートアップガイド」を参照してください。

同期するグループ内のコンピュータについては、同期を設定しているときや (Active Directory と同期する (p. 39)を参照)、「同期のプロパティ」ダイアログボックスで同期のプロパティを編集するときに、自動的に保護できます。

「同期のプロパティ」を編集して、コンピュータを自動保護する方法は、次のとおりです。

1. 「**グループ**」ペインで、自動保護を有効にするコンピュータが所属するグループ (同期ポイント) を選択します。グループを右クリックし、「**同期のプロパティ**」を選択します。
2. 「**同期のプロパティ**」ダイアログボックスで、「**ソフォスのセキュリティソフトを自動インストールする**」チェックボックスを選択します。そして、インストールするソフトウェアを選択します。
   - **Firewall** をコンピュータにインストールする前に、必要なトラフィック、アプリケーション、およびプロセスを許可するようにファイアウォールを構成していることを確認します。デフォルトで、ファイアウォールは有効に設定されるため、必須のトラフィック以外はすべてブロックされます。詳細は、ファイアウォール ポリシー (p. 113)を参照してください。
   - 他社製セキュリティ対策ソフトを自動削除する場合は、「**Third-Party Security Software Detection**」を選択したままにしておいてください。他社製のアップデートツールをアンインストールする必要がある場合は、他社製セキュリティ対策ソフトを削除する (p. 44)を参照してください。
3. ソフトウェアのインストールに使用する管理者アカウントのユーザー名とパスワードを入力します。「**OK**」をクリックします。

後で自動保護を無効にする場合は、「**同期のプロパティ**」ダイアログボックスで、「**ソフォスのセキュリティソフトを自動インストールする**」チェックボックスの選択を外します。

4.5.5 同期のプロパティを表示・編集する

ここでの手順を実行する前に次の項目を確認してください。

- ロールベースの管理を利用する場合、「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。
- 同期しているグループ内のコンピュータを自動で保護する場合は、セキュリティソフトをインストールするための準備をする (p. 44)の説明に従い、コンピュータの準備が済んでいることを確認してください。
- Active Directory の構成が複雑な場合で、ドメインローカルグループやネストされた Active Directory グループを同期するときは、サポートデータベースの文章 122529 の説明に従ってこの機能を有効化してください。

同期のプロパティを表示・編集する方法は次のとおりです。

1. 「**グループ**」ペインで、同期のプロパティを編集するコンピュータが所属するグループ (同期ポイント) を選択します。グループを右クリックし、「**同期のプロパティ**」を選択します。「**同期のプロパティ**」ダイアログボックスが表示されます。
2. 「**Active Directory コンテナ**」フィールドに、グループと同期するコンテナが表示されます。グループを異なるコンテナと同期する場合は、同期を解除してから「**Active Directory の同**

期 ウィザード」をもう一度起動します。詳細は、同期を有効/無効に切り替える (p. 42)およびActive Directory と同期する (p. 39)を参照してください。

3. 「**同期の頻度**」フィールドで、同期の頻度を設定します。デフォルトは 60分です。最短の間隔は5分です。
4. 新しく検出された Windows のクライアントマシンを自動保護し、各グループポリシーを適用するには、「**ソフォスのセキュリティソフトを自動インストールする**」チェックボックスを選択します。「**機能**」パネルで、ウイルス対策がデフォルトで選択されています。ソフォスの他のセキュリティソフトをインストールする場合は、各チェックボックスを選択します。ソフトウェアのインストールに使用する管理者アカウントのユーザー名とパスワードを入力します。

注
自動保護は、Windows のクライアントマシンのみに適用できます。Windows Server OS、Mac OS、Linux、または UNIX が稼動しているコンピュータは自動保護できません。これらのコンピュータは手動で保護する必要があります。詳細は「Sophos Enterprise Console アドバンス スタートアップガイド」を参照してください。

4.5.6 Active Directory と直ちに同期させる

ここでの手順を実行する前に次の項目を確認してください。

- ロールベースの管理を利用する場合、「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。
- 同期しているグループ内のコンピュータを自動で保護する場合は、セキュリティソフトをインストールするための準備をする (p. 44)の説明に従い、コンピュータの準備が済んでいることを確認してください。
- Active Directory の構成が複雑な場合で、ドメインローカルグループやネストされた Active Directory グループを同期するときは、サポートデータベースの文章 122529 の説明に従ってこの機能を有効化してください。

スケジュール設定されている次回の同期予定を待たずに、Enterprise Console のグループ (同期ポイント) と Active Directory のコンテナを直ちに手動で同期することができます。

Active Directory と即時に同期させる方法は次のとおりです。

1. 「**グループ**」ペインで、Active Directory との同期ポイントとなるグループを選択します。グループを右クリックし、「**同期のプロパティ**」を選択します。
2. 「**同期のプロパティ**」ダイアログボックスの内容を適切に変更し、「**OK**」をクリックします。

4.5.7 同期を有効/無効に切り替える

ここでの手順を実行する前に次の項目を確認してください。

- ロールベースの管理を利用する場合、「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。
- 同期しているグループ内のコンピュータを自動で保護する場合は、セキュリティソフトをインストールするための準備をする (p. 44)の説明に従い、コンピュータの準備が済んでいることを確認してください。
- Active Directory の構成が複雑な場合で、ドメインローカルグループやネストされた Active Directory グループを同期するときは、サポートデータベースの文章 122529 の説明に従ってこの機能を有効化してください。

Active Directory との同期の設定を切り替えるには次の手順を実行します。

- 同期を有効にするには、Active Directory と同期する (p. 39)の説明に従い、「**Active Directory の同期 ウィザード**」を実行します。
- 同期を無効にするには、今後、Active Directory と同期させないグループ (同期ポイント) を選択して右クリックし、「**同期の削除**」を選択します。確認メッセージが表示されたら「**はい**」をクリックします。

4.6 Sophos Mobile の URL を設定する

Sophos Mobile は、スマートフォンなどのモバイルデバイス用のデバイス管理ソリューションです。モバイルデバイス上のアプリやセキュリティ設定を管理することで企業データを安全に保ちます。

Enterprise Console でツールバーの「**Sophos Mobile**」ボタンをクリックすると、Sophos Mobile の Web コンソールを開くことができます。この機能を有効にするには、あらかじめ Sophos Mobile の URL を設定しておく必要があります。

1. 「**ツール**」メニューの「**Sophos Mobile の URL の設定**」をクリックします。
2. 「**Sophos Mobile の URL**」ダイアログボックスに Sophos Mobile の Web コンソールの URL を入力し、「**OK**」をクリックします。

5 コンピュータの保護

ソフォスのセキュリティソフトを次のような方法でインストールして、コンピュータを保護することができます。

- コンピュータを自動保護するには、Enterprise Console にあるコンピュータの保護 ウィザードを使用します。コンピュータを自動保護する (p. 45)を参照してください。
- また、Active Directory の同期を使用してコンピュータを自動保護することもできます。Active Directory と同期する (p. 36)を参照してください。
- コンピュータを手動で保護するには、Enterprise Console で必要なソフトウェアの場所を探すことができます。手動でコンピュータを保護するためのインストーラの保存場所を表示する (p. 47)を参照してください。そして、インストール先コンピュータにて、手動でセキュリティソフトをインストールします。

5.1 セキュリティソフトをインストールするための準備をする

ソフトウェアを自動インストールするには、基本的なシステム要件が満たされていることを確認した上で、コンピュータを次のように設定する必要があります。

注
Mac、Linux および UNIX コンピュータに対して自動インストールを行うことはできません。

Active Directory を使用している場合は、グループ ポリシー オブジェクト (GPO) を使ってコンピュータの準備を行うことができます。ワークグループを使用している場合は、ローカルで各コンピュータの準備を行う必要があります。

詳細な手順は、「ソフォス エンドポイント展開ガイド」を参照してください。このガイドをビデオで視聴するには、サポートデータベースの文章 111180 を参照してください。

5.2 他社製セキュリティ対策ソフトを削除する

現在インストールされているセキュリティソフトを削除する場合は、「**コンピュータの保護 ウィザード**」の「**Third-Party Security Software Detection**」オプションを選択してインストールする前に、次の操作を行ってください。

- コンピュータで他社製のウイルス対策ソフトを稼動している場合は、GUI を閉じてください。
- コンピュータで他社製のファイアウォールや HIPS 製品を稼動している場合は、これらのソフトウェアを無効にするか、またはソフォス製品のインストーラの起動を許可するように設定してください。
- 自動的に再インストールが実行されないように、他社製のソフトウェアだけではなく、他社製のアップデートツールも削除する場合は、次の手順を実行してください。なお、コンピュータにアップデートツールがインストールされていない場合、操作は必要ありません。

注
他社製のウイルス対策製品をアンインストールした後は、アンインストールした各コンピュータで再起動を行う必要があります。

注
スタンドアロン製品、または Sophos Central の一機能として、HitmanPro.Alert がインストールされていることがあります。HitmanPro.Alert は、Sophos Enterprise Console からオンプレミス型の管理を適用する前に削除する必要があります。

コンピュータにインストールされている他社製アップデートツールを削除する場合は、「**コンピュータの保護 ウィザード**」の「**Third-Party Security Software Detection**」オプションを選択する前に、設定ファイルを変更してください。

注
コンピュータで他社製のファイアウォールや HIPS 製品を稼動している場合は、同製品用のアップデートツールが今後必要となる可能性があります。詳細は各ベンダの製品ドキュメントを参照してください。

設定ファイルを変更する方法は次のとおりです。

1. CID (セントラル インストール ディレクトリ) で data.zip ファイルを参照します。
2. data.zip から crt.cfg という設定ファイルを展開します。
3. crt.cfg ファイルを開き、「RemoveUpdateTools=0」という行を「RemoveUpdateTools=1」に変更します。
4. 変更を保存し、crt.cfg を data.zip と同じディレクトリに保存します。crt.cfg は、data.zip 内には保存しないでください。次に data.zip が更新されたときに上書きされてしまいます。

これで、「**コンピュータの保護 ウィザード**」を起動して、「**Third-Party Security Software Detection**」を選択すると、変更した設定ファイルによって、他社製のセキュリティ対策ソフトとアップデートツールが削除されます。

5.3 コンピュータを自動保護する

コンソールから各コンピュータの保護を開始する前に、次の項目を実行・確認してください。

- コンピュータを保護する前に、必ず、コンピュータが所属するグループにアップデートポリシーを適用してください。
- セキュリティソフトをインストールするための準備をする (p. 44)の説明に従い、コンピュータにセキュリティソフトを自動でインストールするための準備を行ったことを確認してください。
- ロールベースの管理を利用している場合、各コンピュータを保護するには、「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Mac、Linux および UNIX コンピュータに対して自動インストールを行うことはできません。代わりに手動インストールを行ってください。操作方法は、「Sophos Enterprise Console アドバンス スタートアップガイド」を参照してください。

Active Directory の同期を選択し、コンピュータを自動保護する場合は、次の手順を実行する必要はありません。詳細は、Active Directory と同期する (p. 36)や他の関連トピックを参照してください。

コンピュータを自動保護する方法は次のとおりです。

1. 保護するコンピュータがグループに所属しているかどうかに応じて、次のいずれかの手順を実行してください。
   - 保護するコンピュータが「**グループ外のコンピュータ**」フォルダにある場合は、それらのコンピュータをグループにドラッグします。
   - 既にグループに所属している場合は、保護するコンピュータを選択して右クリックし、「**コンピュータの保護**」をクリックします。

   「**コンピュータの保護 ウィザード**」が表示されます。ウィザードの指示に従います。
2. 「**機能の選択**」ページで、インストールする機能を選択します。

   注
   ソフトウェアに対するシステム要件の詳細は、ソフォス Web サイトの「システム要件」(http://www.sophos.com/ja-jp/products/all-system-requirements) を参照してください。

   ウイルス対策機能など、一部の機能は自動的に選択・インストールされます。また、任意で次の機能をインストールできます。一部の機能については、ライセンスに含まれている場合だけ利用できます。

   - **Firewall**

     コンピュータにファイアウォールをインストールする前に、必要なトラフィック、アプリケーション、およびプロセスを許可するようにファイアウォールを構成していることを確認します。デフォルトで、ファイアウォールは有効に設定されるため、必須のトラフィック以外はすべてブロックされます。詳細は、ファイアウォール ポリシー (p. 113)を参照してください。
   - **Patch**
   - **Exploit Prevention, Sophos Clean**

     ランサムウェアやエクスプロイトからシステムを防御する機能です。お持ちのライセンスに含まれている場合、この機能はデフォルトで選択された状態になっています。

     注
     エクスプロイト対策機能 (と Sophos Clean) が利用できるライセンスにアップグレードしても、既に管理下にあるコンピュータには、エクスプロイト対策機能は自動的にインストールされません。インストールするには、もう一度コンピュータを保護しなおす必要があります。

   - **Third-Party Security Software Detection**

     他社製セキュリティ対策ソフトを自動削除する場合は、「**Third-Party Security Software Detection**」を選択したままにしておいてください。他社製セキュリティ対策ソフトの検出機能は、削除後にインストールする製品と同じ機能を持つソフトウェアのみアンインストールします。他社製のアップデートツールをアンインストールする必要がある場合は、他社製セキュリティ対策ソフトを削除する (p. 44)を参照してください。
3. インストール中に発生した問題はすべて、「**保護のサマリー**」ページの「**保護に関する問題**」カラムに表示されます。インストールで発生した問題に対処するには、Sophos Endpoint Security and Control のインストールに失敗する (p. 225)を参照してください。また、問題が発生したコンピュータで手動インストールを実行するには、「Sophos Enterprise Console アドバンス スタートアップガイド」を参照してください。「**次へ**」をクリックします。
4. 「**アカウント情報**」ページで、選択したソフトウェアのインストールに使用できるアカウントの詳細を入力します。

このアカウントは、通常、ドメイン管理者アカウントです。次の条件を満たしている必要があります。

- 保護するコンピュータへのローカル管理者権限がある。
- 管理サーバーをインストールしたコンピュータにログオンできる。
- **アップデート**ポリシーで指定したプライマリサーバーの場所に対する読み取り権限がある。詳細は、アップデートサーバーを設定する (p. 70)を参照してください。

注

ドメインアカウントを使用している場合は、必ず、ドメイン名¥ユーザー名 という形式でユーザー名を入力してください。

インストール先のコンピュータが同じ Active Directory スキーマ内の異なるドメインにある場合は、代わりに、Active Directory の Enterprise Administrator アカウントを使用してください。

5.4 手動でコンピュータを保護するためのインストーラの保存場所を表示する

Enterprise Console を使ってウイルス対策、ファイアウォール、パッチ評価の機能を自動インストールできないコンピュータがある場合は、手動インストールを行ってください。

インストーラの保存場所を表示する方法は次のとおりです。

1. 「**表示**」メニューの「**インストーラの場所**」をクリックします。
2. 「**インストーラの場所**」ダイアログボックスに、各ソフトウェアのサブスクリプションに対応するインストーラの保存場所、ソフトウェアの対応プラットフォーム、およびソフトウェアのバージョンが表示されます。必要なインストーラの保存場所をメモしてください。

セキュリティソフトを他の OS に手動でインストールする方法については、「Sophos Enterprise Console アドバンス スタートアップガイド」を参照してください。

5.5 ネットワークが保護されているか確認する

ネットワークのセキュリティ ステータスの概要は、ダッシュボードで確認してください。詳細は、ダッシュボードのパネル (p. 4)およびダッシュボードを環境設定する (p. 48)を参照してください。

コンピュータのリストのフィルタ機能を使って、問題が発生しているコンピュータをリストに表示できます。たとえば、ファイアウォールやパッチ評価機能がインストールされていないコンピュータや、対処が必要な警告が発生しているコンピュータを表示できます。詳細は、コンピュータが保護されていることを確認する (p. 48)、コンピュータが最新の状態であることを確認する (p. 49)、および問題が発生しているコンピュータを検出する (p. 49)を参照してください。

また、グループ内のコンピュータすべてがポリシーに準拠しているかを確認することもできます。詳細は、コンピュータがグループ固有のポリシーを使用しているか確認する (p. 32)を参照してください。

5.5.1 ダッシュボードを環境設定する

ロールベースの管理を利用している場合、ダッシュボードを設定するには、「**システム環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ダッシュボードには、未対処の警告、エラー、あるいは前回のアップデート日時に基づいたセキュリティ警報、または緊急ステータス インジケータが表示されます。

警報・緊急レベルは、任意に設定できます。

1. 「**ツール**」メニューで、「**ダッシュボードの環境設定**」をクリックします。
2. 「**ダッシュボードの環境設定**」ダイアログボックスで、「**警報レベル**」および「**緊急レベル**」テキストボックスのしきい値を次のように変更します。

   a) 「**未対処の警告があるコンピュータ**」、「**ソフォス製品エラーのあるコンピュータ**」、「**コンピュータのポリシーと保護**」の各パネルで、各インジケータを「警報」、または「緊急」状態に変える、しきい値を入力します。しきい値に指定する値は、管理対象コンピュータ全体に占める特定の問題のあるコンピュータの割合です。

   b) 「**イベントが発生したコンピュータ**」で、過去 1週間に発生したイベントの件数のしきい値を入力します。このしきい値に達したときにダッシュボードに警告が表示されます。

   c) 「**ソフォスからの最新版の取得**」パネルに、アップデート インジケータの表示を「警報」または「緊急」に変える、しきい値を入力します。この値は、前回ソフォスのサーバーに接続し、アップデートを実行してから経過した時間 (単位: 時間) です。「**OK**」をクリックします。

   しきい値をゼロに指定した場合、最初の警告が発生すると直ちに警報が表示されます。

また、各ダッシュボード・パネルで警報・緊急レベルになった場合、特定の宛先にメール警告を送信するよう設定できます。手順については、警告およびメッセージの設定 (p. 189)を参照してください。

5.5.2 コンピュータが保護されていることを確認する

オンアクセス検索および (インストール済みの場合) ファイアウォールを実行している場合、コンピュータは保護されます。また、完全に保護するためには、ソフトウェアが最新版である必要があります。

注
ファイルサーバーなど、特定の種類のコンピュータでは、オンアクセス検索を実行しないよう指定していることも考えられます。この場合は、スケジュール検索が実行され、そのコンピュータが最新版で保護されていることを確認してください。

コンピュータが保護されているかどうかを確認する方法は次のとおりです。

1. 確認するコンピュータのグループを選択します。
2. グループのサブグループ内のコンピュータをチェックする場合は、ドロップダウンリストから「**このレベル以下**」を選択します。
3. コンピュータのリストの「**ステータス**」タブを開き、「**オンアクセス**」カラムの表示を確認します。
   「アクティブ」と表示されている場合は、そのコンピュータでオンアクセス検索が稼動していることを示します。グレーの盾アイコンが表示されている場合、オンアクセス検索は稼動していません。

4. ファイアウォールをインストール済みの場合は、「**ファイアウォール**」カラムを参照してください。
   「有効」と表示されている場合は、ファイアウォールが有効になっていることを示します。グレーのファイアウォール アイコンと「無効」という文字が表示されている場合は、ファイアウォールが無効になっていることを意味します。
5. アプリケーション コントロール、データコントロール、またはパッチ評価など、他の機能を使っている場合は、各カラムのステータスを確認します。

コンピュータが最新の状態であるかどうかを確認する方法については、コンピュータが最新の状態であることを確認する (p. 49)を参照してください。

コンピュータのリストのフィルタ機能を使って、問題が発生しているコンピュータを検索する方法については、問題が発生しているコンピュータを検出する (p. 49)を参照してください。

5.5.3 コンピュータが最新の状態であることを確認する

推奨方法に従って Enterprise Console を設定した場合、コンピュータはアップデート版を自動的に入手するように設定されています。

コンピュータが最新の状態であることを確認する方法は次のとおりです。

1. 確認するコンピュータのグループを選択します。
2. サブグループ内のコンピュータを確認する場合は、ドロップダウンリストから「**このレベル以下**」を選択します。
3. 「**ステータス**」タブの「**更新状況**」カラムの表示を確認します。または、「**アップデートの詳細**」タブを開きます。
   - 「**更新状況**」カラムに「最新」と表示された場合は、コンピュータが最新の状態であることを意味します。
   - 時計アイコンが表示されている場合、コンピュータは最新版で保護されていません。前回アップデートされた日時が表示されます。

このような最新の状態でないコンピュータのアップデートに関する詳細は、最新版のないコンピュータをアップデートする (p. 78)を参照してください。

5.5.4 問題が発生しているコンピュータを検出する

適切に保護されていないコンピュータや、保護に関する他の問題のあるコンピュータの一覧を表示する方法は次のとおりです。

1. 確認するコンピュータのグループを選択します。
2. 「**表示**」ドロップダウンリストから、「**問題があると思われるコンピュータ**」など、表示するコンピュータを選択します。
   また、エントリの配下にあるサブエントリを選択すると、発生している問題別にコンピュータ (グループポリシーと異なるコンピュータや、未対処の警告のあるコンピュータ、またはインストールエラーが発生したコンピュータなど) を表示できます。
3. このグループにサブグループがある場合は、検索対象を「**このレベルのみ**」または「**このレベル以下**」のどちらかに指定します。
   保護に関する問題のあるコンピュータがすべて表示されます。

コンピュータのリストは、この他に、マルウェア、不要と思われるアプリケーション、または疑わしいファイルなどの検出アイテム名でフィルタリングすることもできます。詳細は、検出アイテム名でコンピュータをフィルタリングする (p. 9)を参照してください。

保護に関する問題の対処方法の詳細は、「トラブルシューティング (p. 223)」セクションのコンピュータでオンアクセス検索が稼動していない (p. 223)やその他のトピックを参照してください。

5.6 警告やエラーに対処する

ウイルス、スパイウェア、疑わしいアイテム、アドウェア、または他の不要と思われるアプリケーションが検出されると、Enterprise Console の「**エンドポイント**」ビューの「**ステータス**」タブに警告アイコンが表示されます。

各警告アイコンの説明は、警告アイコンの説明 (p. 50)を選択してください。各種警告の対処方法は、このセクションの他のトピックを参照してください。

注
ソフトウェアが無効になっている場合や最新版でない場合も、コンソールに警告が表示されます。この詳細は、ネットワークが保護されているか確認する (p. 47)を参照してください。

検出された項目の名前など、警告の詳細については、「**警告とエラーの詳細**」タブをクリックしてください。

アップデートマネージャの警告に関する詳細は、アップデートマネージャを監視する (p. 77)を参照してください。

5.6.1 警告アイコンの説明

アイコン	説明
	赤い警告アイコンが「**警告とエラー**」カラムに表示された場合は、ウイルス、ワーム、トロイの木馬、スパイウェア、または疑わしい動作が検出・検知されたことを意味します。
	黄色い警告アイコンが「**警告とエラー**」カラムに表示された場合は、次のいずれか 1つの問題が発生したことを意味します。 • 疑わしいファイルが検出された。 • アドウェアやその他の不要と思われるアプリケーションが検出された。 • エラーが発生した。 黄色い警告アイコンが「**ポリシーコンプライアンス**」カラムに表示された場合は、グループ内の他のコンピュータと異なるポリシー (複数の場合もあります) が適用されていることを意味します。

コンピュータに複数の警告やエラーがある場合は、優先順位が最も高い警告のアイコンが「**警告とエラー**」カラムに表示されます。警告タイプの優先順位は以下のとおりです (降順)。

1. ウイルス/スパイウェア警告
2. 疑わしい動作警告
3. 疑わしいファイル警告
4. アドウェア/不要と思われるアプリケーション警告
5. ソフトウェアのアプリケーションエラー (インストールエラーなど)

5.6.2 検出されたアイテムに関する警告に対処する

ロールベースの管理を利用している場合、検出されたアイテムをクリーンアップしたり、コンソールから警告を消去するには、「**修復 - クリーンアップ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

コンソールに表示される警告に対処する方法は次のとおりです。

1. 「**エンドポイント**」ビューで、警告を表示するコンピュータ (複数選択可) を選択します。右クリックして、「**警告とエラーの対処**」を選択します。
   「**警告とエラーの対処**」ダイアログボックスが表示されます。
2. 警告に対して実行できるアクションは、警告のクリーンアップステータスによって異なります。「**クリーンアップのステータス**」カラムを参照し、実行するアクションを決定します。

ヒント
警告は各カラムヘッダをクリックすると並び替えられます。たとえば、クリーンアップのステータスで警告を並び替えるには、「**クリーンアップのステータス**」カラムヘッダをクリックします。

クリーンアップのステータス	説明および実行できるアクション
クリーンアップできます	アイテムを削除することができます。削除するには、警告 (複数可) を選択し、「**クリーンアップ**」を選択します。
クリーンアップできないタイプの脅威です	疑わしいファイル、疑わしい動作、または悪質なネットワークトラフィックなど、このタイプのアイテムが検出された場合、コンソールからクリーンアップすることはできません。アイテムを許可またはブロックするかどうかを決める必要があります。アイテムを信頼できない場合は、ソフォスへ解析用サンプルとして提出できます。詳細は、検出されたアイテムに関する情報を表示する (p. 52)を参照してください。
クリーンアップできません	このアイテムはコンソールからクリーンアップできません。アイテムと対処方法の詳細は、検出されたアイテムに関する情報を表示する (p. 52)を参照してください。
システムのフル検索が必要です	クリーンアップは可能ですが、クリーンアップする前に、当該のエンドポイントに対して、システムのフル検索を実行する必要があります。手順については、今すぐコンピュータを検索する (p. 53)を参照してください。
コンピュータの再起動が必要です	アイテムは部分的に削除されていますが、クリーンアップを完了するにはエンドポイントの再起動が必要です。 **注** エンドポイントは、Enterprise Console からではなく、各マシンで再起動する必要があります。
クリーンアップに失敗した	アイテムを削除できなかったことを示します。手動でクリーンアップしなくてはならない場合があります。詳細は、コンピュータを直ちにクリーンアップする (p. 54)を参照してください。

クリーンアップのステータス	説明および実行できるアクション
クリーンアップ実行中 (開始<時刻>)	クリーンアップが進行中であることを示します。
クリーンアップタイムアウト (開始<時刻>)	クリーンアップがタイムアウトしたことを示します。アイテムがクリーンアップされていない可能性があります。この問題は、エンドポイントがネットワークから切断されたり、ネットワークがビジー状態の場合などに、発生することがあります。しばらくしてから、もう一度、アイテムのクリーンアップを試してください。

アイテムを許可する場合は、アドウェアや不要と思われるアプリケーションを認証する (p. 109)、または疑わしいアイテムを認証する (p. 111)を参照してください。

5.6.3 検出されたアイテムに関する情報を表示する

コンソールに表示されるエンドポイントで検出された脅威や他の項目の詳細情報を表示したい場合や、それらの項目に対して実行できるアクションに関するアドバイスが必要な場合は、次のステップを実行してください。

1. 「**エンドポイント**」ビューのコンピュータのリストで対象のコンピュータをダブルクリックします。
2. 「**コンピュータの詳細**」ダイアログボックスで、下にスクロールをして「**未対処の警告とエラー**」セクションを表示します。検出されたアイテムの一覧で、対象の項目名をクリックします。
   ソフォス Web サイトが表示され、ここから各項目に関する解析情報や、対処の方法を参照できます。

注
または、ソフォスの Web サイトの「**セキュリティ解析**」ページ (http://www.sophos.com/ja-jp/threat-center/threat-analyses/viruses-and-spyware.aspx) を開き、ドロップダウンリストから項目の種類を選び、検索フィールドに項目名を入力して検索します。

5.6.4 ランサムウェアの警告を処理する

ロールベースの管理を利用している場合、検出されたアイテムをクリーンアップしたり、コンソールから警告を消去するには、「**修復 - クリーンアップ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

CryptoGuard は、ランサムウェアの警告が発生したエンドポイント上のプロセスをブロックします。ブロックは、警告を消去するまで解除されません。

注
エンドポイントを再起動すると、ブロックが解除されます。感染しているプロセスが起動すると、新たにランサムウェアの警告が発生します。

要確認
検出元のコンピュータで、Sophos Clean を手動で実行する必要があります。実行しないと、コンピュータが警告を発し、当該のプロセスが起動するたびに毎回ブロックされます。

コンソールに表示されるランサムウェアの警告に対処する方法は次のとおりです。

1. 「**エンドポイント**」ビューで、警告を表示するコンピュータ (複数選択可) を選択します。右クリックして、「**警告とエラーの対処**」を選択します。
   「**警告とエラーの対処**」ダイアログボックスが表示されます。
2. 消去するランサムウェアの警告を選択し、「**消去**」をクリックします。
   消去した警告はコンソールに表示されなくなります。プロセスのブロックは解除されます。

5.6.5 コンソールからエンドポイントの警告やエラーを消去する

ロールベースの管理を利用している場合、コンソールから警告やエラーを消去するには、「**修復 - クリーンアップ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

警告に対処する場合、またはコンピュータが安全なことが確実にわかっている場合は、コンソールに表示されている警告アイコンを消去できます。

注
インストールエラーに関する警告を消去することはできません。この種の警告は、Sophos Endpoint Security and Control がコンピュータに正しくインストールされた場合のみに非表示になります。

1. 「**エンドポイント**」ビューで、警告を消去するコンピュータ (複数選択可) を選択します。右クリックして、「**警告とエラーの対処**」を選択します。
   「**警告とエラーの対処**」ダイアログボックスが表示されます。
2. コンソールから警告やソフォス製品エラーを消去するには、「警告またはエラー」タブで、消去する警告やエラーを選択し、「**消去**」をクリックします。
   消去した警告はコンソールに表示されなくなります。

アップデートマネージャの警告をコンソールから消去する方法は、コンソールからアップデートマネージャの警告を消去する (p. 78)を参照してください。

5.7 コンピュータを今すぐ検索、またはクリーンアップする

5.7.1 今すぐコンピュータを検索する

次回のスケジュール検索を待たずに、今すぐコンピュータを検索することができます。

ロールベースの管理を利用している場合、各コンピュータを検索するには「**修復 - アップデートと検索**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

注
Windows、Linux および UNIX を稼動しているコンピュータのみに対して、コンソールから即時にシステムのフル検索を実行できます。

今すぐコンピュータを検索する方法は次のとおりです。

1. コンピュータの一覧からコンピュータを選択するか、「**グループ**」ペインに表示されるグループを選択します。右クリックして、「**システムのフル検索**」を選択します。
   または、「**アクション**」メニューから「**システムのフル検索**」を選択します。
2. 検索を開始するには、「**システムのフル検索**」ダイアログボックスで、検索するコンピュータの詳細を確認し、「**OK**」をクリックします。

注
脅威のコンポーネントがメモリに検出された場合、検索が終了して Enterprise Console に警告が送信されます。これは検索を続行すると脅威が拡散する恐れがあるためです。もう一度検索を実行する前に、必ず脅威をクリーンアップしてください。

5.7.2 コンピュータを直ちにクリーンアップする

Windows を実行しているコンピュータや Mac については、ウイルスに感染していたり、不要と思われるアプリケーションがある場合、即時にクリーンアップできます。

ロールベースの管理を利用している場合、各コンピュータをクリーンアップするには、「**修復 - クリーンアップ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

注
Linux または UNIX コンピュータをクリーンアップするには、コンソールから自動クリーンアップを設定する (オンアクセス検索の自動クリーンアップを設定する (p. 85)を参照) か、またはクリーンアップに失敗した検出アイテムに対処する (p. 55)の説明に従って個別にコンピュータをクリーンアップします。

アイテム (トロイの木馬や不要と思われるアプリケーションなど) が「部分的に検出」された場合、クリーンアップを実行する前に、当該のコンピュータでシステムのフル検索を実行して、部分的に検出されたアイテムのすべてのコンポーネントを検出する必要があります。「**エンドポイント**」ビューのコンピュータのリストで、当該のコンピュータを右クリックし、「**システムのフル検索**」をクリックします。詳細は、アイテムが部分的に検出される (p. 227)を参照してください。

今すぐコンピュータをクリーンアップする方法は次のとおりです。

1. 「**エンドポイント**」ビューのコンピュータのリストで、クリーンアップするコンピュータを右クリックし、「**警告とエラーの対処**」をクリックします。
2. 「**警告とエラーの対処**」ダイアログボックスの「**警告**」タブで、クリーンアップする各アイテムのチェックボックスを選択するか、または、「**すべて選択**」をクリックします。「**クリーンアップ**」をクリックします。

クリーンアップに成功すると、コンピュータのリストで警告は表示されなくなります。

依然として警告が表示される場合は、コンピュータを手動でクリーンアップしてください。詳細は、クリーンアップに失敗した検出アイテムに対処する (p. 55)を参照してください。

注
一部のウイルスをクリーンアップする際にシステムのフル検索が必要になります。この場合、コンピュータ上のすべてのウイルスにクリーンアップが実行されます。完了までに時間がかかることがあります。警告の表示は検索の最後に更新されます。

5.7.3 クリーンアップに失敗した検出アイテムに対処する

コンソールからコンピュータをクリーンアップできない場合は、手動でクリーンアップを実行してください。

1. コンピュータのリストで、感染しているコンピュータをダブルクリックします。
2. 「**コンピュータの詳細**」ダイアログボックスで、下にスクロールをして「**未対処の警告とエラー**」セクションを表示します。検出されたアイテムの一覧で、コンピュータから削除するアイテムの名前をクリックします。
   ソフォス Web サイトが表示され、ここからコンピュータのクリーンアップ方法を参照できます。
3. 各コンピュータで手動でクリーンアップを実行してください。

注
ソフォス Web サイトより、特定のウイルスやワーム用の駆除ツールをダウンロードすることができます。

6 コンピュータのアップデート

6.1 アップデートマネージャを設定する

アップデートマネージャでは、ソフォスの Web サイトからセキュリティソフトを取り込む、自動アップデートを設定できます。アップデートマネージャは、Enterprise Console と同時にインストールされ、Enterprise Console のコンソール画面から管理します。

アップデートマネージャは、複数インストールできます。たとえば、ネットワークが異なる場所に設置されており構成が複雑な場合、離れた場所のネットワークに追加のアップデートマネージャをインストールできます。詳細は、アップデートマネージャを追加する (p. 62)を参照してください。

6.1.1 アップデートマネージャの機能

アップデートマネージャの設定が完了すると、次のタスクが実行されます。

- 設定した一定の頻度で、ソフォスや、社内ネットワーク上のデータ配信用ウェアハウスに接続する。
- 脅威検出データのアップデート版をダウンロードし、管理者がサブスクリプションを設定しているセキュリティソフトを更新する。
- エンドポイントコンピュータへのインストールに適した形式で、更新されたソフトウェアをネットワーク共有 (複数可) に配置する。

アップデートポリシーを適用するなど、コンピュータにインストールされているソフォスのソフトウェアが設定されている場合、ネットワーク共有からコンピュータの自動アップデートを実行する。

6.1.2 アップデートマネージャの環境設定を表示・編集する

ロールベースの管理を利用している場合、アップデートマネージャを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**エンドポイント**」ビューを表示している場合は、ツールバーの「**アップデートマネージャ**」ボタンをクリックし、「**アップデートマネージャ**」ビューを表示します。
2. 一覧から、環境設定を表示、または編集するアップデートマネージャを選択します。右クリックし、「**環境設定の表示/編集**」をクリックします。

   注
   または、アップデートマネージャを選択し、「**アクション**」メニューから、「**アップデートマネージャ**」、「**環境設定の表示/編集**」の順にクリックします。

   「**アップデートマネージャの環境設定**」ダイアログボックスが表示されます。
3. 次のトピックを参照して環境設定を編集します。
   - アップデートマネージャのアップデート元を選択する (p. 57)。
   - ダウンロードするソフトウェアを選択する (p. 58)。

- ソフトウェアの配置場所を指定する (p. 59)。
- アップデートスケジュールを作成・編集する (p. 60)。
- アップデートマネージャのログを設定する (p. 61)。
- アップデートマネージャの自己アップデートを設定する (p. 61)。

アップデートマネージャの警告をコンソールから消去する方法は、コンソールからアップデートマネージャの警告を消去する (p. 78)を参照してください。

アップデートマネージャの設定が完了したら、アップデートポリシーを設定してエンドポイントコンピュータに適用します。

6.1.3 アップデートマネージャのアップデート元を選択する

ロールベースの管理を利用している場合、アップデートマネージャを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

アップデートマネージャで、セキュリティソフトや、アップデート版をダウンロードする場所を選択します。ダウンロードしたソフトウェアやアップデート版は、ここからネットワーク上の各コンピュータに配布されます。

アップデート元は複数選択できます。リストの一番上に表示されるアップデート元がプライマリのアップデート元です。リストの他のアップデート元は、任意で設定する予備のアップデート元で、アップデートマネージャが、プライマリのアップデート元からアップデート版を取得できないときに利用します。

1. 「**エンドポイント**」ビューを表示している場合は、ツールバーの「**アップデートマネージャ**」ボタンをクリックし、「**アップデートマネージャ**」ビューを表示します。
2. アップデート元を選択するには、一覧から対象のアップデートマネージャを選択します。右クリックし、「**環境設定の表示/編集**」をクリックします。
3. 「**アップデートマネージャの環境設定**」ダイアログボックスの「**アップデート元**」タブで、「**追加**」をクリックします。
4. 「**アップデート元の詳細**」ダイアログボックスの「**アドレス**」フィールドに、アップデート元のアドレスを入力します。アドレスには、UNC パスまたは HTTP パスを指定します。

   直接ソフォスから、ソフトウェアとアップデート版をダウンロードする場合は、「**Sophos**」を選択します。
5. 必要に応じて、「**ユーザー名**」と「**パスワード**」フィールドに、アップデート元にアクセスするためのユーザー名とパスワードを入力します。
   - アップデート元に「Sophos」を指定する場合は、ソフォスから入手したダウンロード用アカウントの詳細を入力します。
   - アップデート階層のより上部に位置するアップデートマネージャによって作成されたデフォルトの共有フォルダをアップデート元に指定する場合は、「**ユーザー名**」と「**パスワード**」フィールドは、自動的に入力されます。

     デフォルトのアップデート元共有フォルダは、UNC 共有の ¥¥<コンピュータ名>¥SophosUpdate です。ここで、<コンピュータ名> は、アップデートマネージャをインストールしたコンピュータの名前です。
   - アップデート元にネットワーク上のデフォルト以外の共有フォルダを指定する場合は、当該の共有フォルダへの読み取り権限のあるアカウント情報を入力します。「**ユーザー名**」とドメイン名をあわせて指定する必要がある場合は、ドメイン名¥ユーザー名 という形式で入力してください。
6. プロキシサーバー経由でインターネットにアクセスする場合は、「**プロキシサーバーを使用して接続する**」を選択します。そして、プロキシサーバーの「**アドレス**」と「**ポート**」番号を入力し

ます。プロキシサーバーにアクセスするための「**ユーザー名**」と「**パスワード**」を入力します。「ユーザー名」とドメイン名をあわせて指定する必要がある場合は、ドメイン名¥ユーザー名 という形式で入力してください。「OK」をクリックします。
「**アップデートマネージャの環境設定**」ダイアログボックスに新しいアップデート元が表示されます。

アップデートマネージャを別のコンピュータにインストールしている場合は、インストール済みのアップデートマネージャがソフトウェア/アップデート版をダウンロードする場所が「アドレス」リストに表示されます。このアドレスを当該のアップデートマネージャのアップデート元として選択することもできます。最後に、「**上へ移動**」と「**下へ移動**」ボタンを使って、プライマリアップデート元に設定するアドレスをリストの一番上に移動します。

6.1.4 ダウンロードするソフトウェアを選択する

ロールベースの管理を利用している場合、アップデートマネージャを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

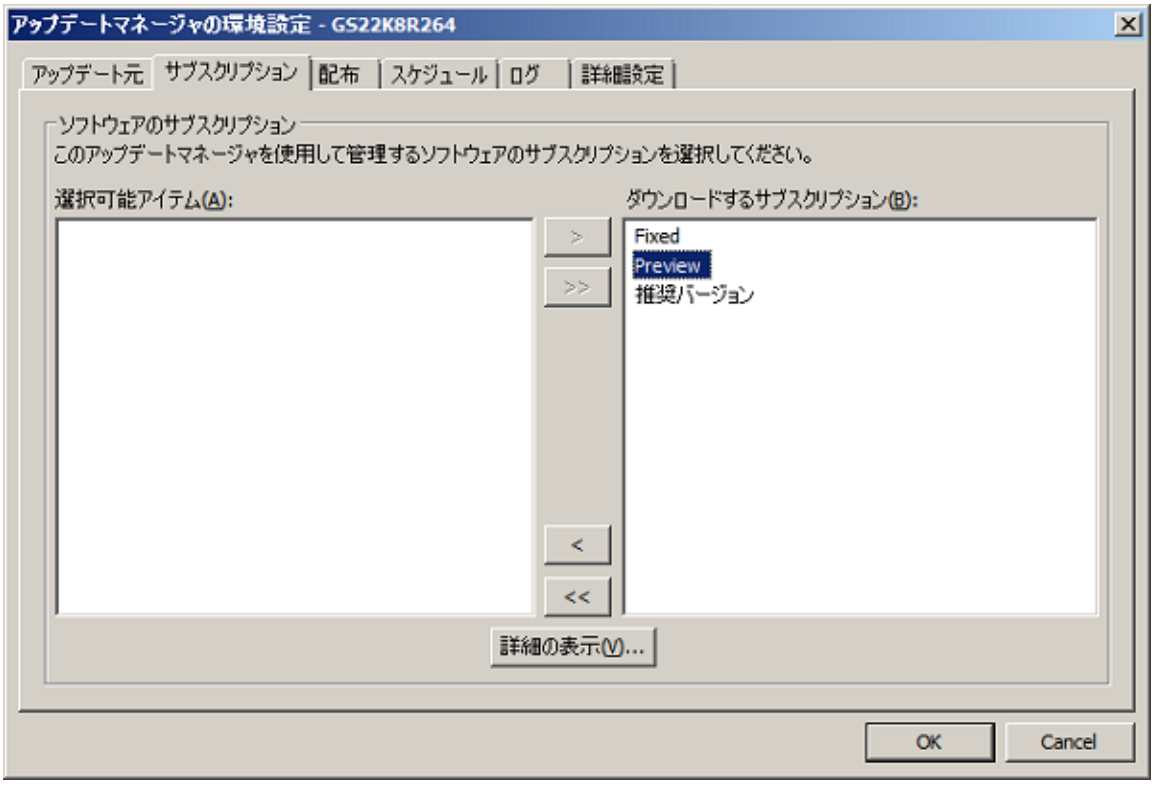
アップデートマネージャで、最新の状態に保つサブスクリプションを選択する必要があります。

1. 「**エンドポイント**」ビューを表示している場合は、ツールバーの「**アップデートマネージャ**」ボタンをクリックし、「**アップデートマネージャ**」ビューを表示します。
2. ダウンロードするソフトウェアを選択するには、一覧から対象のアップデートマネージャを選択します。右クリックし、「**環境設定の表示/編集**」をクリックします。
3. 「**アップデートマネージャの環境設定**」ダイアログボックスの「**サブスクリプション**」タブで、「選択可能アイテム」リストからソフトウェアのサブスクリプションを選択します。
   サブスクリプションに含まれるソフトウェアなどの詳細を表示するには、「**詳細の表示**」をクリックします。
4. 選択したサブスクリプションを「ダウンロードするサブスクリプション」リストに移動するには、「追加」ボタンをクリックします。

   すべてのサブスクリプションを「ダウンロードするサブスクリプション」リストに移動するには、「すべて追加」ボタンをクリックします。



6.1.5 ソフトウェアの配置場所を指定する

ロールベースの管理を利用している場合、アップデートマネージャを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ダウンロードするソフトウェアを選択したら、ネットワーク上のソフトウェアの配置場所を指定します。デフォルトで、ソフトウェアは、UNC 共有の ¥¥<コンピュータ名>¥SophosUpdate に配置されます。ここで、<コンピュータ名> は、アップデートマネージャをインストールしたコンピュータの名前です。

ダウンロードしたソフトウェアは、複数のネットワーク共有フォルダに配布できます。設定するには、選択可能なネットワーク共有フォルダのリストに、既存のフォルダを追加し、次の手順で、アップデート版を配置するフォルダのリストに移動します。アップデートマネージャ用ユーザーアカウント (**SophosUpdateMgr**) に、共有フォルダに対する読み取り権限が与えられていることを確認してください。

注
アップデートマネージャ用ユーザーアカウントは、Enterprise Console をインストールする前に作成したものです。アカウントについての詳細は、「Enterprise Console スタートアップガイド」を参照してください。

ソフトウェアの配置場所を指定する方法は次のとおりです。

1. 「**エンドポイント**」ビューを表示している場合は、ツールバーの「**アップデートマネージャ**」ボタンをクリックし、「**アップデートマネージャ**」ビューを表示します。
2. ソフトウェアを配布するネットワーク共有フォルダを選択するには、一覧から対象のアップデートマネージャを選択します。右クリックし、「**環境設定の表示/編集**」をクリックします。

3. 「**アップデートマネージャの環境設定**」ダイアログボックスの「**配布**」タブで、リストからソフトウェアのサブスクリプションを選択します。
4. 「選択可能アイテム」リストから、ネットワーク共有フォルダを選択し、「>」という追加ボタンをクリックして「アップデート先」リストに移動します。

   デフォルトのネットワーク共有フォルダ ¥¥<コンピュータ名>¥SophosUpdate は、常に、「アップデート先」リストに表示されます。このネットワーク共有フォルダはリストから削除できません。

   「選択可能アイテム」リストには、Enterprise Consoleで認識され、他のアップデートマネージャで使用されていない、すべてのネットワーク共有フォルダが含まれます。

   「選択可能アイテム」リストに既存のネットワーク共有フォルダを追加、またはリストから削除するには、「>」という追加ボタンや、「<」という削除ボタンを使います。
5. ネットワーク共有フォルダの詳細や、書き込みに必要なアカウント情報を入力する場合は、対象のネットワーク共有を選択し、「**環境設定**」をクリックします。「**共有マネージャ**」ダイアログボックスで、説明とアカウント情報を入力します。

   複数の共有フォルダに対して同じアカウント情報を入力する場合は、「アップデート先」リストから共有フォルダを選択し、「**環境設定**」をクリックします。「**複数の共有フォルダの環境設定**」ダイアログボックスで、共有フォルダに対して書き込みを行うときに使うアカウント情報を入力します。

6.1.6 アップデートスケジュールを作成・編集する

ロールベースの管理を利用している場合、アップデートマネージャを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、アップデートマネージャは、10分間隔でソフォスのデータバンクに接続し、**脅威検出データ**に更新がないかチェックを行います。

このアップデート間隔は変更できます。最短の間隔は 5分で、最長の間隔は、1440分 (24時間) です。ソフォスから検出データがリリースされた直後に保護を入手できるよう、脅威検出データのアップデート間隔は、10分に設定することを推奨します。

デフォルトで、アップデートマネージャは、60分間隔でソフォスのデータバンクに接続し、**ソフトウェア**に更新がないかチェックを行います。

このアップデート間隔は変更できます。最短の間隔は 10分で、最長の間隔は、1440分 (24時間) です。

ソフトウェアのアップデート間隔は、毎日 1時間ごとに設定できるほか、曜日を指定したり、曜日ごとに時間帯を分けて異なる間隔を指定するなど、きめ細やかにスケジュールを設定できます。

注
曜日ごとに異なるスケジュールを作成することもできます。各曜日に適用できるスケジュールは1つだけです。

1. 「**エンドポイント**」ビューを表示している場合は、ツールバーの「**アップデートマネージャ**」ボタンをクリックし、「**アップデートマネージャ**」ビューを表示します。
2. アップデートスケジュールを作成するには、一覧から対象のアップデートマネージャを選択します。右クリックし、「**環境設定の表示/編集**」をクリックします。
3. 「**アップデートマネージャの環境設定**」ダイアログボックスの「**スケジュール**」タブで、脅威検出データのアップデート間隔を入力します。
4. ソフトウェアをアップデートする間隔を入力します。

- アップデート間隔を毎日 1時間ごとに設定する場合は、「**アップデート版のチェック**」オプションの「分ごと」欄に間隔を分単位で入力します。
- さらに詳細なスケジュールや、曜日ごとに異なるスケジュールを作成する場合は、「**アップデートをスケジュール設定・管理する**」オプションを選択し、「**追加**」をクリックします。

  「**アップデートスケジュール**」ダイアログボックスで、スケジュールの名前を入力し、曜日とアップデート間隔を選択します。

6.1.7 アップデートマネージャのログを設定する

ロールベースの管理を利用している場合、アップデートマネージャを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**エンドポイント**」ビューを表示している場合は、ツールバーの「**アップデートマネージャ**」ボタンをクリックし、「**アップデートマネージャ**」ビューを表示します。
2. ログを設定するには、一覧から対象のアップデートマネージャを選択します。右クリックし、「**環境設定の表示/編集**」をクリックします。
3. 「**アップデートマネージャの環境設定**」ダイアログボックスの「**ログ**」タブで、ログの保存日数と最大サイズを選択します。

6.1.8 アップデートマネージャの自己アップデートを設定する

ロールベースの管理を利用している場合、アップデートマネージャを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**エンドポイント**」ビューを表示している場合は、ツールバーの「**アップデートマネージャ**」ボタンをクリックし、「**アップデートマネージャ**」ビューを表示します。
2. 自己アップデートを設定するには、一覧から対象のアップデートマネージャを選択します。右クリックし、「**環境設定の表示/編集**」をクリックします。
3. 「**アップデートマネージャの環境設定**」ダイアログボックスの「**詳細設定**」タブで、最新の状態に保つアップデートマネージャのバージョンを選択します。
   たとえば、「Recommended」(推奨バージョン) を選択すると、常に自動的に、ソフォスで「最新バージョン」としてリリースされるアップデートマネージャにアップグレードされます。アップデートマネージャのバージョンが実際に変わります。

6.1.9 今すぐアップデートマネージャでアップデート版をチェックする

ロールベースの管理を利用している場合、ここでのタスクを実行するには「**修復 - アップデートと検索**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

アップデートマネージャの設定を完了すると、設定したスケジュールに従って、アップデート版がチェックされるようになります。アップデート版は、アップデート元からダウンロードされ、自動管理するアップデート版配置用の共有フォルダへ保存されます。アップデートマネージャで、脅威検出データ、エンドポイントコンピュータ用ソフトウェア、およびアップデートマネージャ用ソフトウェアのアップデート版のチェックとダウンロードを、ただちに実行するには、次の手順を実行してください。

1. 「**エンドポイント**」ビューを表示している場合は、ツールバーの「**アップデートマネージャ**」ボタンをクリックし、「**アップデートマネージャ**」ビューを表示します。

2. アップデートマネージャのリストから、アップデートするアップデートマネージャを選択します。右クリックして、「**今すぐアップデート**」をクリックします。

6.1.10 アップデートマネージャに環境設定を適用する

ロールベースの管理を利用している場合、アップデートマネージャを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 「**エンドポイント**」ビューを表示している場合は、ツールバーの「**アップデートマネージャ**」ボタンをクリックし、「**アップデートマネージャ**」ビューを表示します。
2. アップデートマネージャのリストから、環境設定を適用するアップデートマネージャを選択します。右クリックして、「**環境設定の適用**」をクリックします。

6.1.11 アップデートマネージャを追加する

Sophos Update Manager (SUM) は、必ず、Enterprise Console と同じコンピュータにインストールされます。インストールの際に「**カスタム セットアップ**」を選択した場合は、管理サーバーをインストールしたコンピュータにインストールされます。

アップデートマネージャは、1つ以上、ネットワークに追加インストールできます。アップデートマネージャを追加インストールすると、既にインストールされているアップデートマネージャの負荷が削減され、アップデート版の配信が効率化されます。追加のアップデートマネージャは、既にアップデートマネージャがインストールされていないコンピュータにインストールします。

重要
アップデートマネージャと Enterprise Console の管理サーバーを同じコンピュータにインストールしている場合は、アップデートマネージャをアンインストールしないでください。Enterprise Console のすべての機能を使ってネットワークを保護するには、このアップデートマネージャのアップデート元を設定する必要があります。この設定を行うことで、Enterprise Console で必要な更新情報を取得できるようになります。この情報には、エンドポイント用セキュリティソフトの適切なバージョンに関する情報、データコントロール機能で使う新規・更新版のコンテンツ コントロール リスト、新しい管理対象デバイス/アプリケーションのリストなどが含まれます。

追加のアップデートマネージャが、HTTP を通じてソフォスのサーバーや別のアップデートマネージャに接続し、セキュリティソフトをダウンロードできるようにするには、追加のアップデートマネージャをインストールするコンピュータの TCP ポート 80 (送信方向) を開放します。アップデートマネージャが、別のアップデートマネージャの UNC パスに接続してセキュリティソフトをダウンロードできるようにするには、サーバーの送信方向の各ポート (UDP 137、UDP 138、TCP 139、および TCP 445) を解放します。

ネットワーク探索機能が搭載されているバージョンの Windows を実行しているコンピュータの場合、ネットワーク探索機能が無効になっていれば、有効にしてコンピュータを再起動します。

コンピュータでユーザーアカウント制御 (UAC) を有効にしている場合、UAC を無効にし、コンピュータを再起動します。UAC は、アップデートマネージャをインストールし、ソフォス アップデートに登録した後で、有効に設定することができます。

コンピュータがドメインに所属している場合は、ドメイン管理者としてログオンします。

コンピュータがワークグループに所属している場合は、ローカル管理者としてログオンします。

アップデートマネージャのインストーラは、Enterprise Console の管理サーバーがインストールされているコンピュータにあります。保存場所は、¥¥サーバー名¥SUMInstallSet です。インストー

ラの保存場所を表示するには、「**表示**」メニューの「**Sophos Update Manager のインストーラの場所**」をクリックします。

Sophos Update Manager は、Windows のリモートデスクトップ機能を使ってインストールすることもできます。

追加のアップデートマネージャをインストールする方法は次のとおりです。

1. Sophos Update Manager のインストーラ、**Setup.exe** を起動します。インストールウィザードが起動します。
2. ウィザードの「**ようこそ**」ページで、「**次へ**」をクリックします。
3. 「**使用許諾契約**」ページで、使用許諾契約を読んだ後、同意する場合は「**使用許諾契約の条項に同意します**」をクリックして続行します。「**次へ**」をクリックします。
4. 「**インストール先のフォルダ**」ページで、デフォルトのフォルダをそのまま使用するか、または「**変更**」をクリックして新しいインストール先フォルダを入力します。「**次へ**」をクリックします。
5. 「**Sophos Update Manager のアカウント**」ページで、エンドポイントコンピュータが、デフォルトのアップデート用共有フォルダに接続するためのアカウントを選択します。この共有フォルダはアップデートマネージャをインストールすると作成されます。(デフォルトのアップデート元共有フォルダは、¥¥<コンピュータ名>¥SophosUpdate です。ここで、<コンピュータ名> は、アップデートマネージャをインストールしたコンピュータの名前です。)このアカウントには、共有フォルダに対する読み取り権限が必要です。管理者権限は必要ありません。

   デフォルトのユーザーや既存のユーザーを選択したり、新しいユーザーを作成できます。

   ソフトウェアをインストールすると、デフォルトで **SophosUpdateMgr** というアカウントが作成されます。このアカウントには、デフォルトのアップデート用共有フォルダに対する読み取り権限と、アカウント情報を入力せずにログオンできる権限が与えられます。

   後で追加のアップデート用共有フォルダを設定する場合は、既存のアカウントを選択するか、共有に対して読み取り権限を持つ新しいアカウントを作成します。これ以外の場合は、デフォルトで作成されるアカウント、**SophosUpdateMgr** に共有フォルダに対する読み取り権限が与えられていることを確認してください。
6. 「**Sophos Update Manager のアカウント情報**」ページで、前のステップで選択したオプションに応じて、デフォルトユーザー用のパスワード、新しいユーザーのアカウント情報、または既存のアカウントを選択します。

   アカウント用のパスワードは、必ず、パスワードポリシーに適したものを使用してください。
7. 「**プログラムをインストールする準備ができました**」ページにて、「**インストール**」をクリックします。
8. インストールが終了したら、「**完了**」をクリックします。

Sophos Update Manager をインストールしたコンピュータが Enterprise Console の「**アップデートマネージャ**」ビューに表示されます。(「**表示**」メニューの「**アップデートマネージャ**」をクリックします。)

アップデートマネージャを設定するには、アップデートマネージャを選択し、右クリックします。そして、「**環境設定の表示/編集**」をクリックします。

6.1.12 セキュリティソフトを Web サーバーに配置する

各コンピュータから HTTP 経由でアクセスできるように、ソフォスのセキュリティソフトを Web サーバーに配置することもできます。

Web サーバーにセキュリティソフトを配置する方法は次のとおりです。

1. セキュリティソフトのダウンロード先の共有フォルダ (通称、「インストーラの場所」) へのパスを表示する方法は次のとおりです。

   a) Enterprise Console で、「**表示**」メニューの「**インストーラの場所**」をクリックします。

「**インストーラの場所**」ダイアログボックスで、「**場所**」カラムに、各 OS ごとのインストーラの場所が表示されます。

b) CIDs フォルダまでのパス (CIDs は含まない) をメモします。たとえば、次のように入力します。
¥¥サーバー名¥SophosUpdate

2. インストーラの場所 (サブフォルダを含む) を Web サーバーからアクセス可能にします。手順については、ソフォスのサポートデータベースの文章 38238 を参照してください。

6.2 ソフトウェアのサブスクリプションを設定する

ソフトウェアのサブスクリプションは、各プラットフォームに対して、ソフォスのサーバーから定期的にダウンロードする、エンドポイント用ソフトウェアのバージョンを指定するものです。

「**セキュリティソフトのダウンロード**」ウィザードでは、「Recommended」(推奨バージョン) というデフォルトのサブスクリプションが設定されます。このサブスクリプションには、選択したソフトウェアの推奨バージョンが含まれます。

ソフトウェアをサブスクリプションに追加したり、推奨バージョン以外を定期的にダウンロードする場合は、セキュリティソフトのサブスクリプションを設定する (p. 66)の説明に従ってサブスクリプションを設定してください。

Enterprise Console をインストールした後に、ウィザードを完了していない場合は、「セキュリティソフトのダウンロード」ウィザードを起動する (p. 68)を参照してください。

6.2.1 利用可能なアップデート版の種類

各 OS (例: Windows など) に対して、アップデート版の種類やエンドポイントソフトウェアの各種バージョンに対応した、複数のソフトウェアパッケージがあります。ソフォスからダウンロードし、各エンドポイントコンピュータに配布するソフトウェアのパッケージは、サブスクリプションで次のいずれか 1種類のアップデート版を選択して指定します。

アップデート版の種類	説明
Recommended (推奨バージョン)	これはデフォルトパッケージです。このパッケージを使用すると、ソフォスはインストールしたソフトウェアの次の機能を定期的に (通常毎月) アップデートします。 • お客様が発見した問題点の修正。 • 一般使用向けにリリースされた新機能。 Enterprise Console をはじめてインストールして、デフォルト設定で設定すると、このバージョンが指定されます。

アップデート版の種類	説明
Preview (プレビューバージョン)	このパッケージは IT 担当者やセキュリティ管理者向けです。 このバージョンを使用すると、「Recommended」バージョンでリリースされる前に新機能が届けられます。これにより、一般向けにリリースされる前に、テスト環境などで新機能をテストしたり評価したりすることができます。 **注** 「Preview」パッケージのソフトウェアが「Recommended」パッケージの内容と同じである場合もあります。これは、お客様環境でテスト可能な新機能がないことを意味します。
Extended (延長バージョン)	「Extended」バージョンは、ネットワークにアップデート版ソフトウェアをインストールする際の手順が厳格もしくは保守的な環境を対象としています。 このバージョンは、「Recommended」バージョンと同じアップデート版ですが、数か月遅れて届けられます。つまり、ネットワークに製品をインストールする時点では、すでに問題点が発見され、修正されていることを意味します。
Previous Recommended (1つ前の推奨バージョン)	最新「Recommended」パッケージの 1つ前のバージョンです。 新バージョンのソフトウェアを実環境にインストールする前に、少し時間をかけてテスト使用する場合などに、このバージョンは便利です。
Previous Extended (1つ前の延長バージョン)	最新「Extended」パッケージの 1つ前のバージョンです。 新バージョンのソフトウェアを実環境にインストールする前に、少し時間をかけてテスト使用する場合などに、このバージョンは便利です。
固定バージョン	詳細は、固定バージョンのソフトウェアパッケージ (p. 65)を参照してください。

注
今後、パッケージが変更される可能性もあります。現在利用可能なソフトウェアパッケージの詳細は、ソフォスのサポートデータベースの文章 119216 を参照してください。

「**セキュリティソフトのダウンロード**」ウィザードでは、選択したソフトウェアの「Recommended」バージョンを指定するサブスクリプションが設定されます。

通常、実際にダウンロードされるバージョンは、毎月、変わります。実際にダウンロードされたソフトウェアバージョンを確認するには、「**ソフトウェアのサブスクリプション**」ダイアログボックスで、確認するパッケージを選択し、「**詳細**」をクリックします。

6.2.2 固定バージョンのソフトウェアパッケージ

固定バージョンは、脅威検出データで更新されるが、ソフトウェアは毎月リリースされる最新バージョンに更新されないバージョンです。たとえば、Sophos Endpoint Security and Control for Windows の固定バージョンの場合は、「10.3.15 VE3.60.0」などと表示されます。バージョン番号は、3つのバージョン識別子で構成されます。メジャーリリース識別子 (「10」)、マイナーリ

リース識別子 (「3」)、メンテナンスリリース識別子 (「15」)、それに脅威検出エンジンのバージョン (「VE3.60.0」) が付きます。

固定パッケージの使用

デフォルトで、固定バージョンのソフトウェアパッケージの使用は無効化されています (「**ツール > 固定パッケージの使用設定**)。固定パッケージは、「**ソフトウェアのサブスクリプション**」ダイアログに表示されないため、選択することができません。

ヒント
固定バージョンのソフトウェアを使用している場合は、最適な保護が適用されるよう、サブスクリプションを「Recommended」パッケージに変更することを推奨します。ソフトウェアパッケージの詳細は、利用可能なアップデート版の種類 (p. 64) を参照してください。

これまで固定バージョンのソフトウェアパッケージを選択していなかった場合、固定パッケージを選択できるようにするには、「**ツール > 固定パッケージの使用設定**」から設定します。固定パッケージの使用を有効化すると、「**ソフトウェアのサブスクリプション**」ダイアログボックスに固定パッケージが表示され、選択できるようになります。

注
ロールベースの管理を利用している場合、固定パッケージの使用を設定するには、「**システム環境設定**」権限が必要です。

固定パッケージを選択している状態で、固定パッケージの使用を無効化した場合でも、そのパッケージの選択は解除されず、選択を解除するまでダウンロードされ続けます。ただし、他の固定パッケージを表示したり、選択したりすることはできなくなります。

別のコンピュータにも管理コンソールをインストールして使用している場合は、それらのリモートコンソールのいずれかでこの設定を変更すると、すべての管理コンソールに変更が反映されます。ソフォスのサポートデータベース 117348 の手順に従ってレジストリの設定を変更して固定パッケージの使用を有効化した場合は、設定を行ったコンピュータのみにレジストリの設定が反映され、この設定が管理コンソールの設定より優先されます。

固定パッケージのライフサイクル

固定バージョンは、ソフォスからダウンロードが可能な限り、ダウンロードされます。固定バージョンの製品サポートが終了する際は、「**アップデートマネージャ**」ビューで、当該のバージョンのサブスクリプションを指定しているアップデートマネージャの横に警告が表示されます。メール警告が有効になっている場合は、管理者宛てにも警告がメール送信されます。

サブスクリプションに選択した固定バージョンの製品サポートが終了すると、終了する前にサブスクリプションを変更しないと、新しい 固定 Extended パッケージが自動的に選択されます。詳細は、ソフォスのサポートデータベースの文章 121139 を参照してください。

ソフォスのエンドポイント製品のライフサイクルポリシーについて詳細は、ソフォスのサポートデータベースの文章 112580 を参照してください。

6.2.3 セキュリティソフトのサブスクリプションを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ソフトウェアのサブスクリプションを編集するには、「**ポリシー設定 - アップデート**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているアップデートポリシー用のサブスクリプションだけ編集できます。

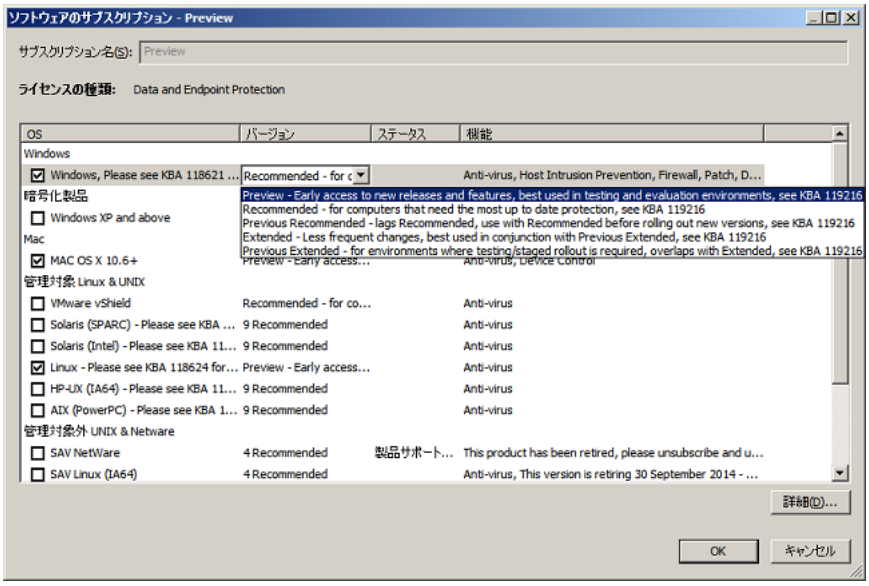
ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

セキュリティソフトのサブスクリプションを設定する方法は次のとおりです。

1. 「**表示**」メニューの「**アップデートマネージャ**」をクリックします。
2. 「**ソフトウェアのサブスクリプション**」ペインで、変更するサブスクリプションをダブルクリックするか、ペイン上部の「**追加**」ボタンをクリックし、新しいサブスクリプションを作成します。

   「**ソフトウェアのサブスクリプション**」ダイアログボックスが表示されます。

   または、既にあるサブスクリプションのコピーを作成するには、コピーするサブスクリプションを選択して右クリックし、「**サブスクリプションの複製**」をクリックします。新しい名前を入力したら、サブスクリプション名をダブルクリックし、「**ソフトウェアのサブスクリプション**」ダイアログボックスを開きます。
3. 「**ソフトウェアのサブスクリプション**」ダイアログボックスで、必要に応じて、サブスクリプションの名前を変更します。
4. ソフトウェアをダウンロードするプラットフォームの種類を選択します。
5. デフォルトで、「Recommended」(推奨バージョン) パッケージに登録しています。デフォルト以外のパッケージを指定することもできます (例: 新機能をプレビューする場合など)。その場合は、パッケージを変更するプラットフォームの横にある「**バージョン**」フィールドをクリックし、続けてもう一度クリックします。利用可能なバージョンのドロップダウンリストから、ダウンロードするバージョンを選択します (例: 「Preview」(プレビューバージョン))。



   その他の利用可能なパッケージについては、利用可能なアップデート版の種類 (p. 64)を参照してください。

ソフトウェアのサブスクリプションを設定したら、サブスクリプションに関するメール警告を設定できます。サブスクリプションに関するメール警告の詳細は、ソフトウェアのサブスクリプションの警告を設定する (p. 189)を参照してください。

新しいソフトウェアのサブスクリプションを作成した場合は、アップデートマネージャの環境設定を表示・編集する (p. 56)の説明に従い、作成したサブスクリプションがアップデートマネージャによってダウンロードされるように設定します。

6.2.4 「セキュリティソフトのダウンロード」ウィザードを起動する

ロールベースの管理を利用している場合、「**セキュリティソフトのダウンロード ウィザード**」を実行するには、「**ポリシー設定 - アップデート**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Enterprise Console をインストールした後に、「**セキュリティソフトのダウンロード ウィザード**」を完了していない場合は、次の手順を実行してください。

- 「**アクション**」メニューの「**セキュリティソフトのダウンロード ウィザードの実行**」をクリックします。

  「**セキュリティソフトのダウンロード ウィザード**」の画面に従い、ソフトウェアの選択とダウンロードを行います。

注
ウィザードの完了後は、「**アクション**」メニューから「**セキュリティソフトのダウンロード ウィザードの実行**」オプションが非表示になります。

6.2.5 サブスクリプションを使用しているアップデートポリシーを表示する

サブスクリプションを使用しているアップデートポリシーを表示する方法は、次のとおりです。

- サブスクリプションを選択して右クリックし、「**サブスクリプションの使用状況の表示**」をクリックします。

  「**ソフトウェアのサブスクリプションの使用状況**」ダイアログボックスに、当該のサブスクリプションを使用しているアップデートポリシーが表示されます。

6.3 アップデートポリシーを設定する

アップデートポリシーを使って、選択したセキュリティソフトのアップデート版を各コンピュータにインストールして最新の状態に保つことができます。Enterprise Console は、アップデート版をチェックし、指定した間隔でコンピュータをアップデートします。

デフォルトのアップデートポリシーを使うと、「Recommended」(推奨バージョン) サブスクリプションで指定されるソフトウェアをインストール、アップデートできます。

デフォルトのアップデートポリシーを変更したり、新しいアップデートポリシーを作成する場合は、これより後のトピックの手順を実行してください。

- サブスクリプションを選択する (p. 69)
- アップデートサーバーを設定する (p. 70)
- アップデートをスケジュール設定する (p. 75)
- 新規インストール用に別のインストール元を設定する (p. 75)
- アップデート活動をログに出力する (p. 76)

注
ロールベースの管理を利用している場合は次の点に注意してください。

- アップデートポリシーを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

6.3.1 サブスクリプションを選択する

ロールベースの管理を利用している場合は次の点に注意してください。

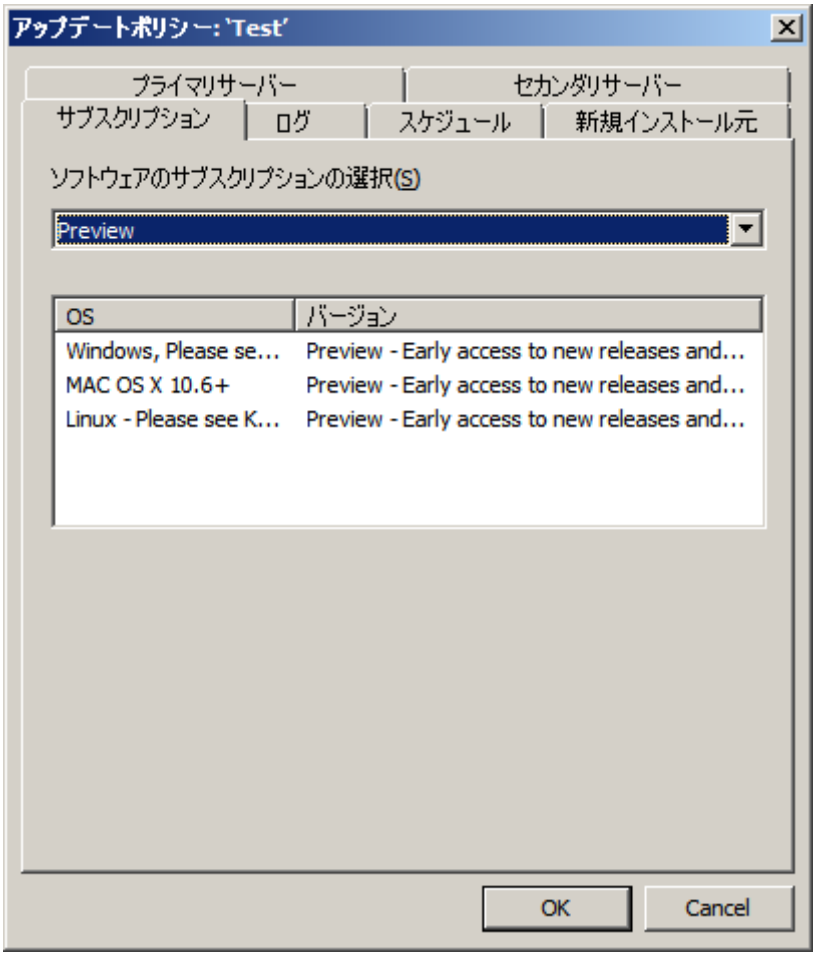
- アップデートポリシーを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

サブスクリプションは、各プラットフォームに対して、ソフォスのサーバーから定期的にダウンロードする、エンドポイント用ソフトウェアのバージョンを指定するものです。デフォルトのサブスクリプションは、Windows 用の最新のソフトウェアを含みます。

サブスクリプションを選択する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのアップデートポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**アップデート**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**アップデートポリシー**」ダイアログボックスで、「**サブスクリプション**」タブをクリックし、最新の状態に保つソフトウェアのサブスクリプションを選択します。



6.3.2 アップデートサーバーを設定する

デフォルトで各コンピュータのアップデート元は、UNC 共有のプライマリロケーション、¥¥<コンピュータ名>¥SophosUpdate です。ここで、<コンピュータ名> は、アップデートマネージャをインストールしたコンピュータの名前です。これ以外にセカンダリロケーションを指定して、移動先でのアップデートのほか、帯域幅の調整を行うこともできます。

エンドポイントコンピュータからプライマリのアップデート元に接続できない場合、セカンダリアップデート元からアップデートを試みます (アップデート元が指定されている場合)。セカンダリアップデート元は、常に指定しておくことを推奨します。

プライマリ アップデート サーバーとセカンダリ アップデート サーバーのロケーションには、ご使用のネットワーク上のアクセス可能なアップデートマネージャの UNC 共有または HTTP URL を指定できます。セカンダリ アップデート サーバーのロケーションは、インターネット (HTTP) 経由でソフォスから直接アップデート版を入手するように設定することもできます。

注
アップデートマネージャの設定内容によっては、配布元となる共有が複数存在する場合もあります。

プライマリサーバー

プライマリサーバーには、自動でデフォルトのプライマリ サーバー ロケーションが設定されます。デフォルトで各コンピュータのアップデート元は、UNC 共有のプライマリロケーション、¥¥<コンピュータ名>¥SophosUpdate です。ここで、<コンピュータ名> は、Sophos Update Manager がインストールされているコンピュータの名前です。

この共有にアクセスするために、Enterprise Console をインストールした際に入力した Sophos Update Manager のアカウント情報がコンピュータで使用されます。Enterprise Console スタートアップガイドで推奨される設定を使用した場合、アカウント名は「SophosUpdateMgr」です。

アカウント情報を変更する必要がある場合は、プライマリサーバーのアカウント情報を変更する (p. 73)を参照してください。

プロキシサーバー経由でアップデート元にアクセスする場合は、「**プロキシの詳細**」をクリックしてプロキシサーバーの詳細を入力してください。

移動先でのアップデートを有効にする場合は、モバイル PC の移動先でのアップデート (p. 71)を参照してください。

帯域幅の制限を有効化して、コンピュータがアップデートを実行する際に使用する帯域幅を制限することもできます。アップデートポリシーの「**プライマリサーバー**」タブで、「**詳細設定**」ボタンをクリックします。「**詳細設定**」ダイアログボックスで、「**使用するバンド幅を制限する**」チェックボックスを選択し、定規コントロールを使用して、Kビット/秒単位で最大バンド幅を指定します。

モバイル PC の移動先でのアップデート

ユーザーによっては、モバイル PC を組織の国内・海外各地のオフィスで使用する場合があります。(モバイル PC 用のアップデートポリシーで) 移動先でのアップデートが有効になっている場合、移動先のモバイル PC は、アップデートの遅れやバンド幅への負荷を最小限に抑えるため、接続しているローカルネットワークの他の (固定) エンドポイントに対してクエリを実行し、最も近くにあるアップデートサーバーのロケーションを探してアップデートしようとします。

移動先のモバイル PC は、接続しているローカルネットワークの固定エンドポイントに対してクエリを実行して、アップデートサーバーのロケーションやアカウント情報を入手します。複数のロケーションが返された場合は、どれが最も近いロケーションか判断し、それを使用します。いずれのロケーションにも接続できない場合、モバイル PC は自身のアップデートポリシーに定義されているプライマリロケーション (接続できない場合はセカンダリロケーション) を使用します。

注
固定コンピュータがモバイル PC にアップデートサーバーのロケーションやアカウント情報を送信する際、パスワードは送信・保管時の両方で曖昧化されます。エンドポイントがアップデートサーバーのロケーションを読み取るためのアカウントには、制限付きアカウントとして、読み取り専用の権限のみを与えるようにしてください。詳細は、ソフトウェアの配置場所を指定する (p. 59)を参照してください。

移動先でのアップデートの詳細は、移動先でのアップデートの仕組み (p. 72)を参照してください。

移動先でのアップデートは、次の環境のみで実行できます。

- 1つの Enterprise Console が、移動先のモバイルPC と固定エンドポイントの両方を管理対象にしている。
- 固定エンドポイントと移動先のモバイル PC で同じソフトウェアのサブスクリプションを使用している。

- モバイル PC に適用済みのアップデートポリシーで、プライマリのアップデート元が指定されている。
- 他社製のファイアウォールがある場合、アップデートサーバーのロケーションのクエリや応答を許可するよう設定されている。通常、UDP ポート 51235 が使用されますが、変更することもできます。詳細は、ソフォスのサポートデータベースの文章 110371 を参照してください。

移動先でのアップデートの有効化は、アップデート元の設定の一環として行います。移動先でのアップデート機能は、頻繁に社内外で移動して使用するマシンのグループのみに対して有効にするようにしてください。移動先でのアップデートを有効にする方法は、プライマリサーバーのアカウント情報を変更する (p. 73)を参照してください。

移動先でのアップデートに関するよくある質問は、ソフォスのサポートデータベースの文章 112830 を参照してください。

移動先でのアップデートの仕組み

移動先でのアップデート機能は、モバイル PC 用の高度なアップデート手法で、モバイル PC のアップデートポリシーに指定されているプライマリ/セカンダリアップデート元だけでなく、「最適な」アップデート元からアップデートを行います。

移動先でのアップデートが有効になっている場合、次のように動作します。

1. モバイル PC を別のロケーションで使用すると、インストールされている Endpoint Security and Control のコンポーネント、Sophos AutoUpdate は、接続先ネットワークのデフォルトのゲートウェイの MAC アドレスが、前回アップデートのときと異なると判定します。その後、近接の AutoUpdate 複数にローカル サブネット経由で ICMP ブロードキャストを行います。デフォルトで UDP ポート 51235 が使用されます。
2. 近接の各 AutoUpdate は、同じポート番号を使用して、自身のアップデートポリシーに基づいて返信します。返信内容には、プライマリのアップデート元のみが含まれます。

   Endpoint Security and Control のインストールは、移動先のアップデートが有効になっているかどうかに関わらず、すべてブロードキャストを待機します。

   返信に含まれる機密情報は難読化され、各フィールドは整合性を保つためにハッシュ化されます。

   返信メッセージの返信時刻は、メッセージストームを避けるためランダム化されます。また、返信メッセージは ICMP ブロードキャストされるので、同じ内容を返信する予定だった他のマシンは、受信したブロードキャストの内容を見て返信しないことを判断できます。
3. AutoUpdate は、受信した複数のアップデート元から「最適な」ロケーションを選び、送信マシンが同じ Enterprise Console で管理されており、サブスクリプション ID がモバイル PC 上の AutoUpdate で使用されているものと一致するかを確認します。

   「最適な」アップデート元は、そこへのアクセスに必要なホップ数に基づいて判断されます。
4. その後、アップデートが実行され、成功した場合、そのアップデート元はキャッシュされます。

   モバイル PC には、サブスクリプション ID が同じで、ホップ数が最小のアクセス可能なアップデート元が、最大 4箇所まで保管されます (保存先ファイル: C:¥Program Files¥Sophos¥AutoUpdate¥data¥status¥iustatus.xml)。

   これらのアップデート元は、AutoUpdate がアップデートを実行するたびにチェックされます。

   注
   アップデートポリシーで指定されるプライマリ/セカンダリアップデート元を再び使用する必要がある場合は (ポリシーで指定されているアップデート元からカスタム設定をロールアウトする場合など)、移動先でのアップデート機能を無効にしてください。

移動先でのアップデートを有効にする

ロールベースの管理を利用している場合は次の点に注意してください。

- アップデートポリシーを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

移動先でのアップデート機能は、頻繁に社内外で移動して使用するマシンのグループのみに対して有効にするようにしてください。

移動先でのアップデートを有効にする方法は次のとおりです。

1. 「**ポリシー**」ペインで、「**アップデート**」をダブルクリックします。次に、変更するアップデートポリシーをダブルクリックします。
2. 「**アップデートポリシー**」ダイアログボックスの「**プライマリサーバー**」タブで、「**移動先でのアップデートを許可する**」チェックボックスを選択します。
3. 「**グループ**」ペインで、変更したアップデートポリシーが適用されているグループを選択します。右クリックし、「**ポリシーの適用 - グループのアップデートポリシー**」を選択します。
   このアップデートポリシーが適用されている各グループに対してこの操作を繰り返します。

注
後でアップデートポリシーで指定されるプライマリ/セカンダリのアップデート元を再び使用する必要がある場合は、移動先でのアップデート機能を無効にしてください。

プライマリサーバーのアカウント情報を変更する

ロールベースの管理を利用している場合は次の点に注意してください。

- アップデートポリシーを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

プライマリサーバーのアカウント情報を変更する方法は次のとおりです。

1. 「**ポリシー**」ペインで、「**アップデート**」をダブルクリックします。次に、変更するアップデートポリシーをダブルクリックします。
2. 「**アップデートポリシー**」ダイアログボックスの「**プライマリサーバー**」タブで、サーバーの接続に使う新しいアカウント情報を入力します。必要に応じて他の項目も変更します。

   注
   プライマリのアップデート元が社内 Web サイト上のフォルダで、Internet Information Services (IIS) を匿名認証で使用している場合でも、「**プライマリサーバー**」タブで、アカウント情報を入力する必要があります。社内 Web サーバーへのアクセスに必要ない場合も含め、「新規インストール元」の UNC 共有フォルダ用のアカウント情報を使用してください。「**プライマリサーバー**」タブで、「**ユーザー名**」と「**パスワード**」フィールドを空白のままにしておくと、コンソールからエンドポイントコンピュータを保護することができません。

3. 「**グループ**」ペインで、変更したアップデートポリシーが適用されているグループを選択します。右クリックし、「**ポリシーの適用 - グループのアップデートポリシー**」を選択します。
   このアップデートポリシーが適用されている各グループに対してこの操作を繰り返します。

セカンダリ アップデート サーバーを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- アップデートポリシーを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

セカンダリのアップデートサーバーのロケーションを設定する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのアップデートポリシーが指定されているか確認してください。

   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**アップデート**」をダブルクリックし、変更するポリシーをダブルクリックします。
3. 「**アップデートポリシー**」ダイアログボックスで、「**セカンダリサーバー**」タブをクリックし、「**セカンダリサーバーの詳細を指定する**」チェックボックスを選択します。
4. 「**アドレス (HTTP、UNC)**」ボックスで、次のいずれかを実行します。
   - HTTP URL またはアップデートサーバー共有の UNC ネットワークパスを入力します。
   - 「**Sophos**」を選択します。

   重要
   HTTP URL、または集中管理するアップデートマネージャで管理していないネットワーク共有フォルダを指定した場合、Enterprise Console は、指定したソフトウェアのサブスクリプションがダウンロード可能かどうかをチェックできません。アドレスに、指定したソフトウェアのサブスクリプションが存在するかどうかを手動で確認する必要があります。手動で確認しないと、コンピュータがアップデートされません。
5. ポリシーに Mac エンドポイントが含まれ、「**アドレス**」フィールドで UNC パスを指定した場合は、「**Mac OS X 用ファイル共有プロトコルの選択**」で、アップデート共有フォルダにアクセスするためのプロトコルを選択してください。
6. 必要に応じて、サーバーへのアクセスに使用するアカウントのユーザー名を「**ユーザー名**」フィールドに入力します。そして、「パスワード」を入力し、確認入力してください。Sophos HTTP の場合、これはソフォスのサブスクリプション アカウント情報です。

   このアカウントには、先ほどアドレスフィールドに入力した共有に対して、読み取り専用のアクセス権限のみが与えられている必要があります。

   注
   「ユーザー名」とドメイン名をあわせて指定する必要がある場合は、ドメイン名¥ユーザー名という形式で入力してください。Windows ユーザーアカウントを確認する方法について、詳細はソフォスのサポートデータベースの文章 11637 を参照してください。
7. バンド幅を制限するには、「**詳細設定**」をクリックします。「**詳細設定**」ダイアログボックスで、「**使用するバンド幅を制限する**」チェックボックスを選択し、定規コントロールを使用して、Kビット/秒単位で最大バンド幅を指定します。
8. プロキシサーバー経由でアップデート元にアクセスする場合は、「**プロキシの詳細**」をクリックしてください。「**プロキシの詳細**」ダイアログボックスで、「**プロキシ経由でサーバーにアクセスする**」チェックボックスを選択します。そして、プロキシサーバーの「**アドレス**」と「**ポート**」番号を入力します。プロキシサーバーにアクセスするための「**ユーザー名**」と「**パスワー**

ド」を入力します。「ユーザー名」とドメイン名をあわせて指定する必要がある場合は、ドメイン名¥ユーザー名 という形式で入力してください。

注
インターネットサービスプロバイダの中には、HTTP リクエストをプロキシサーバーに送信するよう要求するところがあります。

9. 「**OK**」をクリックして、「**アップデートポリシー**」ダイアログボックスを閉じます。
10. 「**グループ**」ペインで、ここで変更したアップデートポリシーを使用するグループを右クリックし、「**ポリシーの適用 > グループのアップデートポリシー**」をクリックします。
    このアップデートポリシーが適用されている各グループに対してこの操作を繰り返します。

6.3.3 アップデートをスケジュール設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- アップデートポリシーを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、各エンドポイントコンピュータは 5分ごとにネットワーク共有内のアップデート版をチェックします。

注
各コンピュータが直接ソフォスからアップデート版をダウンロードする場合、ここで設定するアップデート間隔は適用されません。Sophos PureMessage を稼動しているコンピュータは、アップデート版の有無を 15分ごとにチェックします。Sophos PureMessage を稼動していないコンピュータは、1時間ごとにチェックします。

アップデートの間隔を指定する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのアップデートポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**アップデート**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**アップデートポリシー**」ダイアログボックスの「**スケジュール**」タブで、「**ネットワーク上のソフォス アップデート版の有無を自動チェックする**」を選択します。ソフトウェアをアップデートする間隔 (分単位) を入力します。
4. インターネットへのダイヤルアップ接続で、コンピュータをアップデートする場合は、「**ダイヤルアップ時にアップデート版をチェックする**」を選択します。
   コンピュータをインターネットに接続するたびに、アップデート版のチェックが実行されます。

6.3.4 新規インストール用に別のインストール元を設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- アップデートポリシーを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。

- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、セキュリティソフトは、「**プライマリサーバー**」タブで指定した場所からインストールされ、最新版でアップデートされます。新規インストール用に、これと異なる場所を指定できます。

注
ここでの設定内容は、Windows のみに適用されます。

プライマリサーバーが HTTP (Web) アドレスで、コンソールから各コンピュータにインストールを行う場合は、必ず、新規インストール用のインストール元を指定するようにしてください。

新規インストールを別の場所から行う方法は次のとおりです。

1. 設定するコンピュータのグループに、どのアップデートポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**アップデート**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**アップデートポリシー**」ダイアログボックスの「**新規インストール元**」タブで、「**プライマリサーバーアドレスを使用する**」チェックボックスの選択を外します。そして、使用するインストール元のアドレスを入力します。

6.3.5 アップデート活動をログに出力する

ロールベースの管理を利用している場合は次の点に注意してください。

- アップデートポリシーを設定するには、「**ポリシー設定 - アップデート**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、アップデート活動のログが各コンピュータに記録されます。デフォルトのログの最大サイズは 1MB です。デフォルトのログレベルは「通常」です。

ログの設定を変更する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのアップデートポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**アップデート**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**アップデートポリシー**」ダイアログボックスの「**ログ**」タブで、「**Sophos AutoUpdate のアクティビティをログに出力する**」のチェックを付けたままにします。「**ログの最大サイズ**」フィールドで、ログファイルの最大容量を MB単位で指定します。
4. 「**ログレベル**」フィールドで、「**通常**」または「**詳細**」を選択します。
   詳細ログレベルを指定すると、通常レベルと比較してより多くの活動に関する情報が記録されるので、ログのサイズは急速に大きくなります。したがって、問題が生じた場合のみこの設定を使用するようにしてください。

6.4 アップデートマネージャを監視する

アップデートマネージャのステータスをダッシュボードで確認する

アップデートマネージャのステータスは、**ダッシュボード**の「**アップデート**」パネルに表示されます。ソフォスからの前回のアップデート日時が表示され、経過時間が警報レベルや緊急レベルを超えた場合には警告が表示されます。

注
アップデートマネージャが一時的にアップデートを実行できない場合、ダッシュボードの「**アップデート**」パネルに警告やエラーは表示されません。警告やエラーは、アップデートマネージャの前回アップデートからの経過時間が、ダッシュボードを環境設定する (p. 48)で指定した警報レベルや緊急レベルを超えた場合のみ生成されます。

アップデートマネージャの警告やエラーを確認する

アップデートマネージャの警告やエラーは、「**アップデートマネージャ**」ビューの「**警告**」や「**エラー**」カラムにそれぞれ表示されます。

ソフトウェアの固定バージョンにサブスクリプション登録している場合、同バージョンの製品サポートが終了間近である場合や終了した場合、警告が表示されます。製品ライセンスを変更した場合も警告が表示されます。

アップデートマネージャの警告やエラーを確認する方法は次のとおりです。

1. 「**エンドポイント**」ビューを表示している場合は、ツールバーの「**アップデートマネージャ**」ボタンをクリックし、「**アップデートマネージャ**」ビューを表示します。
2. アップデートマネージャのリストの「**警告**」と「**エラー**」カラムを参照し、問題が発生していないかどうかを確認します。
3. アップデートマネージャの横に警告やエラーが表示されている場合は、アップデートマネージャを右クリックし、「**アップデートマネージャの詳細の表示**」をクリックします。

   「**アップデートマネージャの詳細**」ダイアログボックスに、脅威検出データと、ソフトウェアの前回更新日時、アップデートマネージャで最新版をダウンロードしているサブスクリプション (複数可) のステータス、およびアップデートマネージャのステータスが表示されます。
4. 特定のアップデートマネージャのステータスや、その対策について、詳細は「**説明**」カラムのリンクを参照してください。

サブスクリプション登録している製品の製品サポートが終了間近である、または製品ライセンスを変更したため、新しいライセンスの下で特定の製品を使用できなくなった、などサブスクリプションを確認、変更する必要がある場合は、セキュリティソフトのサブスクリプションを設定する (p. 66)を参照してください。

ライセンスを変更したことによって新しい機能の使用が可能になった場合、新規ポリシーを設定してからでないとその機能を使用できない場合があります。

メール警告に登録する

サブスクリプション登録している製品バージョンの製品サポートが終了間近である場合や終了した場合、またはライセンスを変更したため使用できる機能に変更があった場合などに、指定した受信

者にメール警告を送信するよう設定できます。詳細は、ソフトウェアのサブスクリプションの警告を設定する (p. 189)を参照してください。

6.4.1 コンソールからアップデートマネージャの警告を消去する

ロールベースの管理を利用している場合、コンソールから警告を消去するには、「**修復 - クリーンアップ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

コンソールからアップデートマネージャの警告を消去する方法は次のとおりです。

1. 「**アップデートマネージャ**」ビューで、警告を消去するアップデートマネージャ (複数選択可) を選択します。右クリックして、「**警告の消去**」を選択します。
「**アップデートマネージャ警告**」ダイアログボックスが表示されます。
2. コンソールから警告を消去するには、該当する警告を選択し、「**消去**」をクリックします。
消去した警告はコンソールに表示されなくなります。

6.5 最新版のないコンピュータをアップデートする

ロールベースの管理を利用している場合、各コンピュータをアップデートするには、「**修復 - アップデートと検索**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

アップデートポリシーを設定し、ネットワークに接続しているコンピュータに適用すると、各コンピュータは自動的に最新の状態に保たれます。アップデートに関する問題が発生しない限り、コンピュータを手動でアップデートする必要はありません。

「**エンドポイント**」ビューのコンピュータのリストで、「**ステータス**」タブを開きます。「**更新状況**」カラムに時計アイコンが表示されているコンピュータは、インストールされているセキュリティソフトが最新版ではありません。前回アップデートされた日時が表示されます。

コンピュータに最新版がない原因として、次のいずれかが考えられます。

- コンピュータがサーバーからアップデート版を取得することに失敗した。
- サーバー自体に最新のソフォス製品がない。

問題点を診断し、コンピュータをアップデートする方法は次のとおりです。

1. 「**エンドポイント**」ビューで、最新版のないコンピュータを含むグループを選択します。
2. 「**ステータス**」タブで、「**更新状況**」カラムヘッダをクリックし、更新状況順にコンピュータを並び替えます。
3. 「**アップデートの詳細**」タブをクリックし、「**プライマリサーバー**」カラムを参照します。
各コンピュータのアップデート元ディレクトリが表示されます。
4. 次に、同じディレクトリからアップデートしているコンピュータすべてを順に参照します。
    - 最新版のないコンピュータと、あるコンピュータの両方が存在する場合、各々のコンピュータに問題があることを意味します。コンピュータを選択し、右クリックして、「**今すぐコンピュータをアップデート**」をクリックしてください。
    - 最新版のあるコンピュータが 1台もない場合、ディレクトリに問題があると考えられます。「**表示**」メニューの「**アップデートマネージャ**」をクリックします。最新版がない可能性のあるディレクトリを管理するアップデートマネージャを選択し、右クリックして「**今すぐアップデート**」をクリックします。次に、「**表示**」メニューの「**エンドポイント**」をクリックしま

す。最新版のないコンピュータを選択し、右クリックして、「**今すぐコンピュータをアップデート**」をクリックしてください。

複数のアップデートマネージャがあり、どれが最新版のないディレクトリを管理しているかわからない場合は、「アップデート階層」レポートで各アップデートマネージャが管理している共有フォルダを確認します。「アップデート階層」レポートを表示するには、「**ツール**」メニューの「**レポートの管理**」をクリックします。「**レポートの管理**」ダイアログボックスで、「**アップデート階層**」を選択し、「**実行**」をクリックします。「アップデートマネージャが管理する共有フォルダ」のセクションを確認します。

7 ポリシーの設定

7.1 ウイルス対策および HIPS ポリシー

ウイルス対策および HIPSポリシーでは次の設定が可能です。

- ユーザーがコピー、移動、または開こうとしたファイルに、既知・未知のウイルス、トロイの木馬、ワーム、またはスパイウェアが含まれている場合に、これらのアイテムを自動的に検出する。
- アドウェアや他の不要と思われるアプリケーションを検索する。
- 疑わしいファイルやルートキットを検索する。
- 悪質なネットワークトラフィック (エンドポイントコンピュータと、ボットネットやその他のマルウェア攻撃に関わっている C&C サーバー間の通信) を検知する。
- ウイルスや他の脅威が発見されると直ちにコンピュータを自動クリーンアップする。

  自動クリーンアップの設定の変更に関する詳細は、オンアクセス検索の自動クリーンアップを設定する (p. 85)を参照してください。
- システムで起動しているプログラムの動作を解析する。

  詳細は、動作監視 (p. 95)を参照してください。
- 指定した日時にコンピュータを検索する。

  詳細は、スケジュール検索を作成する (p. 89)を参照してください。

各コンピュータのグループに対して異なる検索設定を適用できます。検索の環境設定についての詳細は、次のトピックを参照してください。

- オンアクセス検索を環境設定する (p. 82)
- スケジュール検索を環境設定する (p. 90)

注
Sophos Labs は検索を実行するファイルを独自に制御できます。最適な保護機能環境を提供するために、特定のファイルタイプの検索を追加したり、削除したりすることがあります。

Mac、Linux、または UNIX コンピュータに適用されない検索およびクリーンアップのオプションについての詳細は、Mac、Linux、UNIX に適用されない設定 (p. 80)を参照してください。

Sophos Anti-Virus for VMware vShield に適用されない検索やクリーンアップのオプションについて詳細は、ソフォスのサポートデータベースの文章 121745 を参照してください。Sophos Anti-Virus for VMware vShield バージョン 2.x については、「Sophos Anti-Virus for VMware vShield 設定ガイド」もあわせて参照してください。 www.sophos.com/ja-jp/support/documentation/sophos-anti-virus-for-vmware-vshield

7.1.1 Mac、Linux、UNIX に適用されない設定

Windows コンピュータでは、すべての種類の検索およびクリーンアップを Enterprise Console で完全に管理できるのに対して、Mac、Linux、または UNIX では、適用されない設定がいくつかあります。

Mac OS X

Mac 環境に適用するウイルス対策および HIPS ポリシーの設定についての詳細は、ソフォスのサポートデータベースの文章 118859 を参照してください。

Linux

次の自動クリーンアップオプションは、Linux コンピュータでは適用されず無視されます。

オンアクセス検索の自動クリーンアップオプション

- **アクセスを拒否し、デフォルトの場所に移動する**
- **アクセスを拒否し、次の場所に移動する**

スケジュール検索の自動クリーンアップオプション

- **デフォルトの場所に移動する**
- **次の場所に移動する**

自動クリーンアップ設定についての詳細は、スケジュール検索の自動クリーンアップを設定する (p. 91)、およびスケジュール検索の自動クリーンアップ設定 (p. 92)を参照してください。

Linux 環境に適用されるウイルス対策および HIPS ポリシーの設定についての詳細は、ソフォスのサポートデータベースの文章 117344 を参照してください。

UNIX

- Enterprise Console では、UNIX コンピュータのオンアクセス検索は実行できません。

  スケジュール検索、警告、ログ、およびアップデートは、Enterprise Console で一括設定が可能です。

  注
  これらの機能には、Enterprise Console では設定できないパラメータもあります。このようなパラメータは、Sophos Anti-Virus コマンドライン インターフェースを使って、各 UNIX コンピュータでローカル設定してください。パラメータは Enterprise Console では無視されます。

  また、オンデマンド検索も、Sophos Anti-Virus コマンドライン インターフェースを使って、各 UNIX コンピュータでローカル設定できます。

  その他のパラメータ設定や Sophos Anti-Virus for UNIX のローカル設定についての詳細は、「Sophos Anti-Virus for UNIX 環境設定ガイド」を参照してください。

- 次のスケジュール検索の自動クリーンアップオプションは、UNIX コンピュータでは適用されず無視されます。

  — **デフォルトの場所に移動する**

  — **次の場所に移動する**

  スケジュール検索の自動クリーンアップのオプションに関する詳細は、スケジュール検索の自動クリーンアップ設定 (p. 92)を参照してください。

UNIX 環境に適用されるウイルス対策および HIPS ポリシーの設定についての詳細は、ソフォスのサポートデータベースの文章 117344 を参照してください。

7.1.2 オンアクセス検索

オンアクセス検索のベストプラクティス

ここではオンアクセス検索を最適な設定で使用するための推奨事項について説明します。

オンアクセス検索のデフォルト設定は、保護機能とシステムパフォーマンスのバランスが考慮されているため、この設定の使用を推奨します。オンアクセス検索の推奨設定について、詳細はソフォス サポートデータベースの文章 114345 を参照してください。(http://www.sophos.com/ja-jp/support/knowledgebase/114345.aspx)

ソフォスのセキュリティソフトの使用や管理に関するベストプラクティスについて、「Sophos Enterprise Console ポリシー設定ガイド」を参照することを推奨します。ソフォスの製品ドキュメントは次のサイトから入手可能です。 http://www.sophos.com/ja-jp/support/documentation

オンアクセス検索を環境設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

注意
特定の暗号化ソフトがインストールされている場合、オンアクセス検索でウイルスが検出されないことがあります。コンピュータのスタートアップ プロセスを変更し、オンアクセス検索が開始するとファイルが復号化されるように設定してください。暗号化ソフトがインストールされている環境でのウイルス対策および HIPS ポリシーの使用について、詳細はソフォスのサポートデータベースの文章 12790 を参照してください。

オンアクセス検索を設定するには次の操作を行ってください。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンアクセス検索**」パネルで、「**オンアクセス検索を有効にする**」の横にある「**環境設定**」をクリックします。
5. オンアクセス検索の動作を変更するには、「**ファイル検索のタイミング**」パネルで、以下の説明に従ってオプションを選択します。

オプション	説明
読み取ったとき	• ファイルをコピー、移動、開いたときに検索を実行します。

オプション	説明
	• プログラムを起動したときに検索を実行します。
名前の変更	ファイル名を変更したときに検索を実行します。
書き込んだとき	ファイルを保存、作成したときに検索を実行します。

6. 「**検索するアイテム**」パネルで、次の説明に従ってオプションを設定します。

オプション	説明
アドウェアや不要と思われるアプリケーション	• アドウェアはポップアップ メッセージなど広告を表示するプログラムで、ユーザーの生産性やシステム効率に影響を与える可能性があります。 • 不要と思われるアプリケーションは、悪質ではないものの一般的に企業ネットワークには不適切と考えられているアプリケーションです。
疑わしいファイル	疑わしいファイルは、通常マルウェアで見られる (ただしマルウェアには限定されない) 特徴 (動的にデータを展開するコードを含むなど) を持ちます。しかし、それは、ファイルが新種のマルウェアとして検出されるには至りません。 **注** このオプションは、 Sophos Endpoint Security and Control for Windows のみに適用されます。

7. 「**その他の検索オプション**」パネルで、次の説明に従ってオプションを設定します。

オプション	説明
ブートセクタが感染しているドライブへのアクセスを許可する	感染している起動可能なリムーバブルメディアまたはデバイス (ブータブル CD、フロッピーディスク、または USB メモリなど) へのアクセスを許可します。 このオプションはソフォス テクニカルサポートから指示があった場合のみに使います。
圧縮ファイル内を検索する	アーカイブファイルや圧縮ファイルを管理対象コンピュータにダウンロードしたり、管理対象コンピュータからメール送信したりする前に、その中身を検索します。

オプション	説明
	しかしながら、検索スピードが著しく低下するため、このオプションを**無効**に設定することを推奨します。 このオプションが無効になっていても、ユーザーはアーカイブや圧縮ファイル内の脅威から保護されます。マルウェアの可能性があるアーカイブや圧縮ファイルのコンポーネントは、以下のようにオンアクセス検索でブロックされます。 • 圧縮ファイルから解凍したファイルをユーザーが開くと検索が実行されます。 • ダイナミック圧縮ユーティリティ (PKLite、LZEXE、Diet) を使って圧縮されたファイルの検索が実行されます。
システムメモリを検索する	コンピュータのシステムメモリ (OS が使用するメモリ) に潜むマルウェアを検出するバックグラウンド検索を毎時間実行します。

オンアクセス検索を有効/無効に切り替える

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、Sophos Endpoint Security and Control は、ユーザーがファイルにアクセスしようとするとマルウェア検索を実行し、ファイルが感染していない場合のみアクセスを許可します。

Exchange サーバーや、パフォーマンス低下の恐れがある他のサーバーにおいて、オンアクセス検索を無効にするケースもあります。この場合は、サーバーを特定のグループに配置し、次の手順に従って、そのグループに適用されているウイルス対策および HIPS ポリシーを変更してください。

オンアクセス検索を有効/無効に切り替える方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのウイルス対策および HIPS ポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
3. 「**オンアクセス検索**」パネルで、「**オンアクセス検索を有効にする**」チェックボックスを選択するか、または選択を外します。

重要
サーバーでオンアクセス検索を無効にした場合は、該当する各コンピュータにてスケジュール検索を設定することを推奨します。スケジュール検索の設定方法については、スケジュール検索を作成する (p. 89)をご覧ください。

オンアクセス検索の自動クリーンアップを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、Sophos Endpoint Security and Control は、ウイルスや他の脅威が発見されるとすぐにコンピュータを自動的にクリーンアップします。自動クリーンアップの設定は、次の説明に従って変更できます。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンアクセス検索**」パネルで、「**オンアクセス検索を有効にする**」の横にある「**環境設定**」をクリックします。
5. 「**オンアクセス検索の設定**」ダイアログボックスで「**クリーンアップ**」タブをクリックします。
6. オンアクセス検索の自動クリーンアップ設定 (p. 85)の説明に従ってオプションを設定します。

オンアクセス検索の自動クリーンアップ設定

ウイルス/スパイウェア

「**ウイルス/スパイウェアを含むアイテムを自動クリーンアップする**」チェックボックスを選択するか、または選択を外します。

クリーンアップに失敗した場合のアイテムへの対処方法も指定できます。

- **アクセス拒否のみ**
- **削除する**
- **アクセスを拒否し、デフォルトの場所に移動する**
- **アクセスを拒否し、次の場所に移動する (UNC フルパスで指定)**

注
「**アクセスを拒否し、デフォルトの場所に移動する**」および「**アクセスを拒否し、次の場所に移動する**」の設定内容は、Linux または UNIX コンピュータには適用されません。

疑わしいファイル

注
ここでの設定内容は、Windows コンピュータのみに適用されます。

疑わしいファイルが検出された場合の対処方法も指定できます。

- **アクセス拒否のみ**
- **削除する**
- **アクセスを拒否し、デフォルトの場所に移動する**
- **アクセスを拒否し、次の場所に移動する (UNC フルパスで指定)**

オンアクセス検索のファイル拡張子を指定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

オンアクセス検索の対象にするファイル拡張子を指定できます。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンアクセス検索**」パネルで、「**オンアクセス検索を有効にする**」の横にある「**環境設定**」をクリックします。
5. 「**拡張子**」タブをクリックし、次のようにオプションを設定します。

オプション	説明
すべてのファイルを検索する	ファイルの拡張子に関わらず、すべてのファイルを検索します。このオプションを有効にすると、「**拡張子**」タブにある他のオプションは無効になります。 すべてのファイルを検索するとコンピュータのパフォーマンスに影響を与えるため、このオプションは、週に一度のスケジュール検索だけで実行することを推奨します。
実行ファイルなど感染の可能性があるファイルのみを検索する	• 拡張子が実行ファイル形式のファイルすべて (.exe、.bat、.pif など)、または感染の恐れがあるファイル (.doc、.chm、.pdf など) を検索します。

オプション	説明
	• すべてのファイルの構造をすばやくチェックし、実行ファイル形式の場合、検索します。
追加で検索するファイル拡張子	ファイルの種類を追加するには、「**追加**」をクリックして、「**拡張子**」ボックスに拡張子を入力します (例: PDF)。任意の一文字を表すワイルドカード文字「?」を使用できます。 ファイルの種類を検索の対象から外すには、リストからファイルの拡張子を選択し、「**削除**」をクリックします。 ファイルの種類を変更するには、リストからファイルの拡張子を選択し、「**編集**」をクリックします。
拡張子のないファイルも検索する	拡張子のないファイルはマルウェアである可能性があるので、このオプションを選択したままにしておくことを推奨します。
除外	オンアクセス検索から特定のファイルの種類を除外するには、「**追加**」をクリックして、「**拡張子**」ボックスに拡張子を入力します (例: PDF)。 ファイルの種類を再び検索の対象にするには、リストからファイルの拡張子を選択し、「**削除**」をクリックします。 ファイルの種類を変更するには、リストからファイルの拡張子を選択し、「**名前の変更**」をクリックします。

オンアクセス検索の対象から項目を除外する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

オンアクセス検索の対象から項目を除外することができます。

注
これらのオプションは、Windows、Mac OS X および Linux コンピュータのみに適用されます。

Enterprise Console では、UNIX コンピュータのオンアクセス検索は実行できません。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。

2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
3. 「**オンアクセス検索**」パネルで、「**環境設定**」ボタンをクリックします。
4. 「**Windows での除外**」、「**Mac での除外**」、または「**Linux/UNIX での除外**」タブをクリックします。項目をリストに追加するには、「**追加**」をクリックして、「**アイテムの除外**」ダイアログボックスにフルパスを入力します。

   除外できる項目の種類は、コンピュータの OS によって異なります。詳細は、検索の対象から除外できる項目 (p. 105)を参照してください。

   ローカルドライブに保存されていないファイルを除外するには、「**リモートファイルを除外する**」チェックボックスを選択します。信頼できる場所に保存されているリモートファイルへのアクセス速度を高める場合などに、この項目を選択してください。

重要
「**Windows での除外**」タブで「**リモートファイルを除外する**」を選択すると、メールクライアント、Web ブラウザ、IM (インスタント メッセージング) クライアントなどの監視対象アプリケーションを使用してネットワーク内の場所からアップロードまたは添付されたファイルは、データコントロールで検索されません。データコントロールでは、Sophos Anti-Virus オンアクセス スキャナ (InterCheck ™) と同じ除外設定が使用されます。したがって、リモートファイルの検索が無効になっている場合、すべてのリモートファイルはデータコントロールによるチェックを受けないことになります。ストレージデバイスの監視はこの制限の対象ではありません。

Windows で検索から除外する項目の一覧をファイルにエクスポートした後、それを別のポリシーにインポートすることができます。詳細は、オンアクセス検索から除外する項目をインポートまたはエクスポートする (p. 88)を参照してください。

オンアクセス検索から除外する項目をインポートまたはエクスポートする

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Windows でオンアクセス検索から除外する項目の一覧をファイルにエクスポートした後、それを別のポリシーにインポートすることができます。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンアクセス検索**」パネルで、「**オンアクセス検索を有効にする**」の横にある「**環境設定**」をクリックします。
5. 「**Windows での除外**」タブで、「**エクスポート**」または「**インポート**」をクリックします。

7.1.3 オンデマンド検索とスケジュール検索

「**ウイルス対策および HIPS**」ポリシーの「**オンデマンド検索**」パネルでは次の項目を設定できます。

- スケジュール検索の設定。
- 検索オプションの設定。すべてのタイプのオンデマンド検索に対する拡張子や除外、各コンピュータにおけるすべてのスケジュール検索、システムのフル検索、デフォルトのオンデマンド検索など。

スケジュール検索を作成する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

指定した日時に Sophos Endpoint Security and Control でコンピュータを検索するには、スケジュール検索を作成してください。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンデマンド検索**」パネルの「**スケジュール検索の設定・管理**」で、「**追加**」をクリックします。
   「**スケジュール検索の設定**」ダイアログボックスが表示されます。
5. 「**検索名**」ボックスに、検索名を入力します。
6. 「**検索するアイテム**」で、検索するアイテムのチェックボックスを選択します。デフォルトでは、すべてのローカルハードディスクおよびマウントされた UNIX ファイルシステムが検索されます。
7. 「**検索のタイミング**」で、検索を実行する曜日のチェックボックスを選択します。
8. 検索を実行する時刻を指定するには、「**追加**」をクリックします。
   - 時刻を変更するには、「**検索を実行する時間**」リストで時刻を選択し、「**編集**」をクリックします。
   - 時間を削除するには、「**検索を実行する時間**」リストで時刻を選択し、「**削除**」をクリックします。

注
脅威のコンポーネントがメモリに検出された場合で、当該の検索に対して自動クリーンアップを設定していないときは、検索が終了して Enterprise Console に警告が送信されます。これは検索を続行すると脅威が拡散する恐れがあるためです。もう一度検索を実行する前に、必ず脅威をクリーンアップしてください。

検索およびクリーンアップの設定を変更するには、次のトピックを参照してください。

- スケジュール検索を環境設定する (p. 90)
- オンアクセス検索の自動クリーンアップを設定する (p. 85)

スケジュール検索を環境設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

スケジュール検索を環境設定する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**スケジュール検索の設定・管理**」リストで検索を選択し、「**編集**」をクリックします。
5. 「**スケジュール検索の設定**」ダイアログボックスで、「**環境設定**」をクリックします。
6. 「**検索するアイテム**」パネルで、次の説明に従ってオプションを設定します。

オプション	説明
アドウェアや不要と思われるアプリケーション	• アドウェアはポップアップ メッセージなど広告を表示するプログラムで、ユーザーの生産性やシステム効率に影響を与える可能性があります。 • 不要と思われるアプリケーションは、悪質ではないものの一般的に企業ネットワークには不適切と考えられているアプリケーションです。
疑わしいファイル	疑わしいファイルは、通常マルウェアで見られる (ただしマルウェアには限定されない) 特徴 (動的にデータを展開するコードを含むなど) を持ちます。しかし、それは、ファイルが新種のマルウェアとして検出されるには至りません。 **注** この設定は、 Sophos Endpoint Security and Control for Windows のみに適用されます。
ルートキット	ルートキットは、コンピュータのユーザーや管理者から、悪意のあるオブジェクト (プロセス、ファイル、レジストリキー、ネット

オプション	説明
	ワークポート) の存在を隠すために使われるトロイの木馬またはテクノロジーです。

7. 「**その他の検索オプション**」パネルで、次の説明に従ってオプションを設定します。

オプション	説明
圧縮ファイル内を検索する	アーカイブやその他の圧縮ファイルのコンテンツを検索します。 検索時間が大幅に増加するので、スケジュール検索時には、アーカイブファイル内を検索することは推奨しません。代わりに、オンアクセス検索 (読み取ったとき、および書き込んだとき) を実行してネットワークを保護することを推奨します。解凍していないアーカイブ内のマルウェア コンポーネントは、読み取ったときまたは書き込んだときに実行されるオンアクセス検索機能により、アクセス時にブロックされます。 少数のコンピュータ上のアーカイブすべてをスケジュール検索する場合は、次の手順で実行することを推奨します。 • 専用のスケジュール検索を作成します。 • 「**環境設定 > オンデマンド検索の設定**」ダイアログボックスの「**拡張子**」タブで、検索する拡張子のリストに圧縮ファイルの拡張子のみを追加します。 • 「**すべてのファイルを検索する**」が無効になっていることを確認します。 これにより、検索時間を最小限に抑えつつ、アーカイブファイルを検索できます。
システムメモリを検索する	コンピュータのシステムメモリ (OS が使用するメモリ) に潜むマルウェアを検出します。
低いプライオリティで検索を実行する	Windows Vista 以降では、低いプライオリティでスケジュール検索を実行し、ユーザーが実行するアプリケーションへの影響を最小限に抑えることができます。

デフォルトのスケジュール検索の設定の調整について、詳細はソフォスのサポートデータベースの文章 63985 を参照してください。

スケジュール検索の自動クリーンアップを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、Sophos Endpoint Security and Control は、ウイルスや他の脅威が発見されるとすぐにコンピュータを自動的にクリーンアップします。自動クリーンアップの設定は、次の説明に従って変更できます。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**スケジュール検索の設定・管理**」リストで検索を選択し、「**編集**」をクリックします。
5. 「**検索・クリーンアップ設定内容の変更**」の横にある「**環境設定**」をクリックします。
   「**検索・クリーンアップ設定**」ダイアログボックスが表示されます。
6. 「**クリーンアップ**」タブをクリックします。
7. オンアクセス検索の自動クリーンアップ設定 (p. 85)の説明に従ってオプションを設定します。

スケジュール検索の自動クリーンアップ設定

ウイルス/スパイウェア

「**ウイルス/スパイウェアを含むアイテムを自動クリーンアップする**」チェックボックスを選択するか、または選択を外します。

クリーンアップに失敗した場合のアイテムへの対処方法も指定できます。

- **ログのみを生成する**
- **削除する**
- **デフォルトの場所に移動する**
- **次の場所に移動する (UNC フルパスで指定)**

注

- 実行ファイルは移動することで実行される可能性が低くなります。
- 複合感染の各コンポーネントを自動的に移動することはできません。

アドウェアや不要と思われるアプリケーション

「**アドウェアや不要と思われるアプリケーションを自動クリーンアップする**」を選択します。

注

- ここでの設定内容は、Windows コンピュータのみに適用されます。

疑わしいファイル

疑わしいファイルが検出された場合の対処方法も指定できます。

- **ログのみを生成する**
- **削除する**

- **デフォルトの場所に移動する**
- **次の場所に移動する (UNC フルパスで指定)**

注

- ここでの設定内容は、Windows コンピュータのみに適用されます。
- 実行ファイルは移動することで実行される可能性が低くなります。
- 複合感染の各コンポーネントを自動的に移動することはできません。

オンデマンド検索とスケジュール検索のファイル拡張子を指定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

オンデマンド検索とスケジュール検索の対象にするファイル拡張子を指定できます。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンデマンド検索**」パネルで、「**環境設定**」をクリックします。
   「**オンデマンド検索の設定**」ダイアログボックスが表示されます。
5. 「**拡張子**」タブで、次のようにオプションを設定します。

オプション	説明
すべてのファイルを検索する	ファイルの拡張子に関わらず、すべてのファイルを検索します。このオプションを有効にすると、「**拡張子**」タブにある他のオプションは無効になります。 すべてのファイルを検索するとコンピュータのパフォーマンスに影響を与えるため、このオプションは、週に一度のスケジュール検索だけで実行することを推奨します。
実行ファイルなど感染の可能性があるファイルのみを検索する	• 拡張子が実行ファイル形式のファイルすべて (.exe、.bat、.pif など)、または感染の恐れがあるファイル (.doc、.chm、.pdf など) を検索します。 • すべてのファイルの構造をすばやくチェックし、実行ファイル形式の場合、検索します。
追加で検索するファイル拡張子	ファイルの種類を追加するには、「**追加**」をクリックして、「**拡張子**」ボックスに拡張子

オプション	説明
	を入力します (例: PDF)。任意の一文字を表すワイルドカード文字「?」を使用できます。 ファイルの種類を検索の対象から外すには、リストからファイルの拡張子を選択し、「**削除**」をクリックします。 ファイルの種類を変更するには、リストからファイルの拡張子を選択し、「**編集**」をクリックします。
拡張子のないファイルも検索する	拡張子のないファイルはマルウェアである可能性があるので、このオプションを選択したままにしておくことを推奨します。
除外	スケジュール検索から特定のファイルの種類を除外するには、「**追加**」をクリックして、「**拡張子**」ボックスに拡張子を入力します (例: PDF)。 ファイルの種類を再び検索の対象にするには、リストからファイルの拡張子を選択し、「**削除**」をクリックします。 ファイルの種類を変更するには、リストからファイルの拡張子を選択し、「**名前の変更**」をクリックします。

スケジュール検索用の拡張子の設定の詳細は、ソフォスのサポートデータベースの文章 63985 を参照してください。

オンデマンド検索やスケジュール検索の対象から項目を除外する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

オンデマンド検索やスケジュール検索の対象から項目を除外することができます。

注
スケジュール検索に対する「除外されたアイテム」の設定は、コンソールから実行するシステムのフル検索と、ネットワーク上のコンピュータで実行する「ローカルディスクの検索」にも適用されます。詳細は、今すぐコンピュータを検索する (p. 53)を参照してください。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。

3. 「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。「**オンデマンド検索**」パネルで、「**環境設定**」をクリックします。
4. 「**Windows での除外**」、「**Linux/UNIX での除外**」、または「**Mac での除外**」タブをクリックします。項目をリストに追加するには、「**追加**」をクリックして、「**アイテムの除外**」ダイアログボックスにフルパスを入力します。

   除外できる項目の種類は、コンピュータの OS によって異なります。詳細は、検索の対象から除外できる項目 (p. 105)を参照してください。

Windows で検索から除外する項目の一覧をファイルにエクスポートした後、それを別のポリシーにインポートすることができます。詳細は、オンアクセス検索から除外する項目をインポートまたはエクスポートする (p. 88)を参照してください。

Windows でのオンデマンド検索やスケジュール検索の除外項目をインポート/エクスポートする

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Windows でオンデマンド検索やスケジュール検索から除外する項目の一覧をファイルにエクスポートした後、それを別のポリシーにインポートすることができます。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。

   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンデマンド検索**」パネルで、「**環境設定**」をクリックします。
5. 「**Windows での除外**」タブで、「**エクスポート**」または「**インポート**」をクリックします。

7.1.4 動作監視

Sophos Behavior Monitoring は、オンアクセス検索の一機能で Windows コンピュータを未知の「ゼロデイ脅威」および疑わしい動作から保護します。

ランタイム検知では実行前に検出できないセキュリティ脅威が阻止されます。動作監視機能は次のランタイム検知技術で脅威をインターセプトします。

- 悪意のある/疑わしい動作の検知
- Malicious Traffic Detection (MTD - 悪質なトラフィックの検知)
- バッファオーバーフローの検知

悪意のある/疑わしい動作の検知

疑わしい動作の検知は、ソフォスのホスト侵入防止システム (HIPS) を駆使して、コンピュータで実行されているすべてのプログラムの動作を動的に解析し、悪意を持つ可能性のある動作を検知・

ブロックします。疑わしい動作の中には、コンピュータの再起動時にウイルスの自動実行を可能にするレジストリの変更などがあります。

疑わしい動作の検知は、すべてのシステムのプロセスを監視し、レジストリへの疑わしい書き込みやファイルの複製など、アクティブなマルウェアがないかどうかを検知します。この機能を設定し、管理者に警告を送信および/またプロセスをブロックできます。

悪意のある動作の検知は、コンピュータで実行されているすべてのプログラムの動作を動的に解析し、既知の悪質な動作を検知・ブロックします。

Malicious Traffic Detection (MTD - 悪質なトラフィックの検知)

Malicious Traffic Detection (MTD - 悪質なトラフィックの検出) は、エンドポイントコンピュータと、ボットネットやその他のマルウェア攻撃に関わっているコマンド アンド コントロール サーバー間の通信を検知します。

注
Malicious Traffic Detection 機能を使用するには、Sophos Live Protection を有効化してオンラインのデータベース検索と必要なデータの取得を行う必要があります。(デフォルトで、Sophos Live Protection は有効になっています。)

バッファオーバーフローの検知

バッファオーバーフローの検知はゼロデイ攻撃を防御するうえで重要な機能です。

システム上で実行されているプログラムの動作を動的に分析し、バッファーオーバーフローによる、それらのプロセスを悪用する動きを検知します。OS およびアプリケーションのセキュリティの脆弱性を狙った攻撃が検知されます。

動作監視を有効/無効に切り替える

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、動作監視は有効になっています。

動作監視を有効/無効に切り替える方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのウイルス対策および HIPS ポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンアクセス検索**」パネルで、「**動作監視を有効にする**」チェックボックスを選択/選択解除します。

悪意のある動作を検知する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

悪意のある動作の検知は、コンピュータで実行されているすべてのプログラムの動作を動的に解析し、既知の悪質な動作を検知・ブロックします。

デフォルトで、悪意のある動作の検知は有効になっています。

悪意のある動作の検知、レポートの設定を変更する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのウイルス対策および HIPS ポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンアクセス検索**」パネルで、「**動作監視を有効にする**」チェックボックスが選択されていることを確認します。
5. 「**動作監視を有効にする**」の横にある「**環境設定**」をクリックします。
6. 「**動作監視の環境設定**」ダイアログボックスで次の操作を行います。
   - 悪意のある動作をブロックし、管理者に警告を送信するには、「**悪意のある動作を検知する**」チェックボックスを選択してください。
   - 悪意のある動作を無効にするには、「**悪意のある動作を検知する**」チェックボックスを選択から外します。

     注
     悪意のある動作の検知を無効にすると、疑わしい動作の検知も無効になります。なお、悪質なトラフィックの検知は、**無効化**されないことに注意してください。

悪質なトラフィックを検知する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

  詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。
- Malicious Traffic Detection 機能を使用するには、Sophos Live Protection を有効にする必要があります。(デフォルトで、Sophos Live Protection は有効になっています。)

Malicious Traffic Detection (MTD - 悪質なトラフィックの検出) は、エンドポイントコンピュータと、ボットネットやその他のマルウェア攻撃に関わっているコマンド アンド コントロール サーバー間の通信を検知します。

注
悪質なトラフィックの検知には、Sophos Anti-Virus オンアクセススキャナ (InterCheck ™) と同じ除外設定が使用されます。オンアクセス検索の対象から項目を除外する方法の詳細は、オンアクセス検索の対象から項目を除外する (p. 87)を参照してください。

悪質なトラフィックの検知は、Enterprise Console 5.3 以降の新規インストールに対して、デフォルトで有効になっています。Enterprise Console の旧バージョンからアップグレードした場合は、悪質なトラフィックの検知機能を使用するには、有効化する必要があります。

悪質なトラフィックの検知の設定を変更する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのウイルス対策および HIPS ポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンアクセス検索**」パネルで、「**動作監視を有効にする**」チェックボックスが選択されていることを確認します。
5. 「**動作監視を有効にする**」の横にある「**環境設定**」をクリックします。
6. 「**動作監視の環境設定**」ダイアログボックスで、「**悪意のある動作を検知する**」チェックボックスが選択されていることを確認します。
7. 悪質なトラフィックの検知を有効/無効に切り替えるには、「**悪質なトラフィックを検知する**」チェックボックスを選択/選択解除します。

疑わしい動作を検知する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

疑わしい動作の検知は、すべてのシステムのプロセスを監視し、レジストリへの疑わしい書き込みやファイルの複製など、アクティブなマルウェアがないかどうかを検知します。この機能を設定し、管理者に警告を送信および/またプロセスをブロックできます。

デフォルトで、疑わしい動作は検知されレポートされますが、ブロックはされます。

疑わしい動作の検知、レポートの設定を変更する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのウイルス対策および HIPS ポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンアクセス検索**」パネルで、「**動作監視を有効にする**」チェックボックスが選択されていることを確認します。
5. 「**動作監視を有効にする**」の横にある「**環境設定**」をクリックします。

6. 「**動作監視の環境設定**」ダイアログボックスで、「**悪意のある動作を検知する**」チェックボックスが選択されていることを確認します。
   - 疑わしいプロセスをブロックし、管理者に警告を送信するには、「**疑わしい動作を検知する**」チェックボックスを選択し、「**疑わしい動作を警告するが、ブロックしない**」チェックボックスを選択から外します。
   - 管理者に警告を送信するが、疑わしいプロセスをブロックしない場合は、「**疑わしい動作を検知する**」チェックボックスと「**疑わしい動作を警告するが、ブロックしない**」チェックボックスの両方を選択します。

最高の保護レベルに設定するため、疑わしいファイルの検索を有効にすることを推奨します。詳細は、オンアクセス検索を環境設定する (p. 82)を参照してください。

バッファオーバーフローを検知する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

バッファオーバーフローの検知は、システム上で実行されているプログラムの動作を動的に分析し、バッファーオーバーフローを利用したプロセスを悪用する動きを検知します。

デフォルトで、バッファオーバーフローは検知され、ブロックされます。

バッファオーバーフロー攻撃の検知、レポートの設定を変更する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのウイルス対策および HIPS ポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**オンアクセス検索**」パネルで、「**動作監視を有効にする**」チェックボックスが選択されていることを確認します。
5. 「**動作監視を有効にする**」の横にある「**環境設定**」をクリックします。「**動作監視の環境設定**」ダイアログボックスで次の操作を行います。
   - バッファオーバーフローをブロックし、管理者に警告を送信するには、「**バッファオーバーフローを検知する**」チェックボックスを選択し、「**警告するが、ブロックしない**」チェックボックスを選択から外します。
   - バッファオーバーフローをブロックせず、管理者に警告だけ送信するには、「**バッファオーバーフローを検知する**」チェックボックスと「**警告するが、ブロックしない**」チェックボックスの両方を選択します。

7.1.5 Sophos Live Protection

Sophos Live Protection は、オンラインベースのテクノロジーを駆使し、疑わしいファイルが脅威であるかを瞬時に解析し、ウイルス対策および HIPS ポリシーで設定されているアクションを実行します。

誤検知のリスクを抑え、高い精度で新種マルウェアを検出します。既知のマルウェアに関する最新データをリアルタイムに照会することが特長です。新種マルウェアとして検出された場合、ソフォスから脅威定義ファイルのアップデート版を数秒内に受信できます。

Sophos Live Protection の機能を最大限に活用するには、次のオプションを有効に設定する必要があります。

- **Live Protection を有効にする**

  エンドポイントコンピュータのオンアクセス検索機能が検出した疑わしいファイルが、問題のないファイルか、または悪意のあるファイルか、ローカルの脅威定義ファイル (IDE ファイル) に基づいて判断できない場合は、チェックサムなどのファイルの特徴をソフォスに送信して、解析に役立てることができます。オンラインベースのチェックでは、疑わしいファイルがソフォスラボのデータベースと照合されます。ファイルが未感染または悪質であると判断された場合、結果がローカルコンピュータに返信され、ファイルのステータスが自動的に更新されます。

  重要
  Malicious Traffic Detection 機能とダウンロードレピュテーション機能を使用するには、SophosLabs のオンラインデータベースにリアルタイムに照会して最新の脅威データやレピュテーションデータを取得するために、Live Protection を有効化する必要があります。

- **オンデマンド検索での Live Protection を有効にする**

  オンアクセス検索と同じクラウドベースのチェックをオンデマンド検索でも実行する場合は、このオプションを選択します。

- **サンプルファイルをソフォスに自動送信する**

  悪意のあるファイルである可能性があるものの、ファイルの特徴のみからは悪意のあるファイルと判定できない場合、Sophos Live Protection で、ソフォスへのサンプルファイルの送信が要求されます。Sophos Live Protection が有効になっている場合、ソフォスに当該のファイルのサンプルがなければ、ファイルが自動的にソフォスに送信されます。

  ソフォスは、このようなサンプルファイルの送信を通じて、誤検出のリスクを抑えたマルウェア検出率の継続的な向上に取り組んでいます。

  注
  サンプルの最大サイズは 10MB です。サンプルをアップロードする際のタイムアウトは 30秒です。速度の遅いネットワーク (56Kbps 未満) 経由でサンプルを自動送信することは推奨しません。

重要
ご使用の Web フィルタリング ソリューションで、ファイルデータ送信先のソフォスのドメインが信頼できるドメインに指定されている必要があります。詳細は、サポートデータベースの文章 62637 を参照してください (http://www.sophos.com/ja-jp/support/knowledgebase/62637.aspx)。

WS1000 Web Appliance などのソフォス Web フィルタリング ソリューションをご使用の場合、ソフォスのドメインは信頼できるドメインに既に指定されているので、何も操作は必要ありません。

Sophos Live Protection を有効/無効に切り替える

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Sophos Live Protection では、SophosLabs のデータベースの最新データを照会して疑わしいファイルがチェックされます。

デフォルトで、Sophos Live Protection は、チェック用のファイルデータ (チェックサムなど) をソフォスに送信しますが、解析用のサンプルファイルは送信しません。Sophos Live Protection の機能を最大限に活用するには、サンプルファイルの送信オプションを選択する必要があります。

Sophos Live Protection のオプションを有効/無効に切り替える方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのウイルス対策および HIPS ポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**ウイルス対策および HIPS ポリシー**」ダイアログボックスで、「**Sophos Live Protection**」ボタンをクリックします。
4. 「**Sophos Live Protection**」ダイアログボックスで次の操作を行います。
   - 「**Live Protection を有効にする**」チェックボックスを選択するか、または選択を外します。これにより、オンアクセス検索の Live Protection がオン/オフに切り替わります。

     重要
     Malicious Traffic Detection 機能とダウンロードレピュテーション機能を使用するには、SophosLabs のオンラインデータベースにリアルタイムに照会して最新の脅威データやレピュテーションデータを取得するために、Live Protection を有効化する必要があります。

   - 「**オンデマンド検索での Live Protection を有効にする**」チェックボックスを選択するか、または選択を外します。これにより、オンデマンド検索の Live Protection がオン/オフに切り替わります。
   - 「**サンプルファイルをソフォスに自動送信する**」チェックボックスを選択するか、または選択を外します。

     サンプルファイルは、Live Protection が有効化されている場合のみ送信できます。

     注
     Live Protection を実行するためにサンプルファイルがソフォスに送信されると、チェックサムなどのファイルデータも同時に送信されます。

7.1.6 Web Protection

Web Protection は、Web サイトの脅威に対する保護機能を強化します。含まれる機能は次のとおりです。

- ライブ URL フィルタリング
- ダウンロードしたコンテンツのスキャン

- ダウンロードしたファイルのレピュテーションのスキャン

ライブ URL フィルタリング

ライブ URL フィルタリングは、マルウェア感染サイトへのアクセスをブロックします。ソフォスのオンラインデータベースをリアルタイムで照会し、感染サイトかどうかを判定します。

注
ユーザーがアクセスすることで組織が法的責任を問われる可能性がある Web サイトへのアクセスなど、ユーザーにアクセスを許可する Web サイトをより詳細にコントロールする場合は、Web コントロール機能を使用してください。詳細は、Web コントロール ポリシー (p. 177)を参照してください。

コンテンツスキャン

コンテンツスキャンは、インターネット (またはイントラネット) からダウンロードしたデータやファイルを検索し、悪意のあるコンテンツをプロアクティブに検出します。感染サイトデータベースに登録されていないものも含め、コンテンツがホストされている場所に関わらずスキャンを実行できます。

ダウンロードレピュテーション

ダウンロードのレピュテーションは、ファイルの古さ、提供元、発生する頻度、詳細なコンテンツ解析、およびその他の特徴を基に算出されます。

注
ダウンロードレピュテーション機能は、Windows 7 以降のみに対応しています。

ユーザーがレピュテーションの低いファイルまたは不明なファイルをダウンロードしようとすると、デフォルトで警告が表示されます。このようなファイルはダウンロードしないことを推奨します。ファイルの提供元や発行元を信頼する場合は、ファイルのダウンロードを選択してください。選択したアクションとファイルの URL は、検索ログに記録されます。

注
ダウンロードのレピュテーションは、SophosLabs のクラウドデータベースにあるデータに基づいて算出されます。データベースを照会してデータを取得するには、Sophos Live Protection が有効になっている必要があります。(デフォルトで、Sophos Live Protection は有効になっています。)

ダウンロードレピュテーションについて詳細は、サポートデータベースの文章 121319 を参照してください。

Web Protection の設定

デフォルトで、Web Protection は有効になっています。つまり、悪意のある Web サイトへのアクセスはブロックされ、ダウンロードされたコンテンツはスキャンされ、ダウンロードされたファイルのレピュテーションはチェックされます。

Web Protection の設定とその変更方法の詳細は、Web Protection のオプションを設定する (p. 103)を参照してください。

対応している Web ブラウザ

Web Protection は次の Web ブラウザに対応しています。

- Internet Explorer
- Microsoft Edge
- Google Chrome
- Firefox (ダウンロードレピュテーションは非対応)
- Safari (ダウンロードレピュテーションは非対応)
- Opera

対応していないブラウザ経由でアクセスした Web コンテンツはフィルタされず、ブロックされません。

Web Protection のイベント

悪意のある Web サイトへのアクセスがブロックされるとイベントがログに記録され、「Web - イベントビューア」またはイベントが発生したエンドポイントコンピュータの「**コンピュータの詳細**」に表示されます。Web コントロール機能を使用すると、Web Protection のイベントと Web コントロールのイベントの両方が、「Web - イベントユーザー」および「**コンピュータの詳細**」に表示されます。詳細は、Web のイベントを表示する (p. 205)および最新の Web のイベントを表示する (p. 207)を参照してください。

Web Protection のオプションを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Web Protection を有効/無効に切り替える方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのウイルス対策および HIPS ポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
4. 「**ウイルス対策および HIPS ポリシー**」ダイアログボックスで、「**Web Protection**」ボタンをクリックします。
5. 「**Web Protection**」ダイアログボックスの「**マルウェア対策**」の下で、「**悪意のある Web サイトへのアクセスブロック**」を「**有効**」または「**無効**」に選択して、悪意のある Web サイトへのアクセスをブロックしたり、ブロックを解除したりします。このオプションはデフォルトで有効になっています。
   特定の Web サイトを認証する詳細は、Web サイトを認証する (p. 112)を参照してください。

6. ダウンロードしたデータやファイルのスキャンを有効または無効にするには、「**コンテンツスキャン**」の横で「**オンアクセス検索の設定と同じ**」、「**有効**」または「**無効**」を選択します。
   デフォルトでは、「**オンアクセス検索の設定と同じ**」が指定されており、オンアクセス検索の有効/無効設定が、コンテンツスキャンにも適用されます。
7. レピュテーションの低いまたは不明なファイルをユーザーがダウンロードしようとした場合のアクションを変更するには、「**ダウンロードレピュテーション**」下の「**アクション**」を「**ユーザーに通知**」(デフォルト) または「**ログのみを生成する**」に指定してください。

   注
   ダウンロードレピュテーション機能を使用するには、Sophos Live Protection を有効にする必要があります。(デフォルトで、Sophos Live Protection は有効になっています。)

   - 「**ユーザーに通知**」を選択すると、ユーザーがレピュテーションの低いファイルをダウンロードしようとするたびに、警告が表示され、ダウンロードをブロックするか、または許可するかどうか確認を求めるメッセージが表示されます。このようなファイルはダウンロードしないことを推奨します。ファイルの提供元や発行元を信頼する場合は、ファイルのダウンロードを選択してください。ダウンロードのブロックと許可のどちらを選択したか、およびファイルの URL は、検索ログに記録されるほか、Enterprise Console の Web のイベントログとしても記録されます。
   - 「**ログのみを生成する**」を選択した場合、警告は表示されません。また、ダウンロードが許可され、検索ログに記録されるほか、Enterprise Console の Web のイベントログとしても記録されます。
8. レピュテーションスキャンのレベルは、「**しきい値**」に対して「**推奨**」(デフォルト) または「**高レベル**」を選択します。
   - 「**推奨**」を選択すると、ユーザーがレピュテーションの低いまたは不明なファイルをダウンロードしようとするたびに警告が表示され、また、ログとイベントが作成されます。
   - 「**高レベル**」を選択すると、ユーザーがレピュテーションの低いファイルや不明なファイルのほか、レピュテーションが中レベルのファイルをダウンロードしようとするたびに警告が表示され、また、ログとイベントが作成されます。

7.1.7 検索するファイルの種類と除外

Sophos Endpoint Security and Control では、デフォルトで、ウイルスに感染しやすい種類のファイルに対して検索が実行されます。デフォルトで検索されるファイルの種類は、OS によって異なるだけでなく、製品アップデート時にも変更されることがあります。

デフォルトで検索されるファイルの種類の一覧を表示するには、該当する OS を稼動しているコンピュータから、Sophos Endpoint Security and Control または Sophos Anti-Virus を開き、「拡張子」環境設定ページを開きます。

また、別の種類のファイルを検索したり、特定の種類のファイルを検索から除外したりすることもできます。

Windows

Windows コンピュータでデフォルトで検索されるファイルの種類の一覧を表示するには、次の手順を実行します。

1. Sophos Endpoint Security and Control を開きます。
2. 「**ウイルス対策および HIPS**」で、「**ウイルス対策および HIPS の環境設定**」をクリックし、さらに「**拡張子＆除外リスト (オンデマンド検索)**」をクリックします。

Windows コンピュータで、別の種類のファイルを検索したり、特定の種類のファイルを検索から除外したりする設定の詳細は、次のトピックを参照してください。

- オンアクセス検索のファイル拡張子を指定する (p. 86)
- オンデマンド検索とスケジュール検索のファイル拡張子を指定する (p. 93)

Mac OS X

Sophos Anti-Virus for Mac OS X のオンアクセス検索では、すべてのファイル拡張子に対して検索が実行されます。スケジュール検索の設定を変更するには、オンデマンド検索とスケジュール検索のファイル拡張子を指定する (p. 93)を参照してください。

Linux または UNIX

Linux コンピュータでは、「Sophos Anti-Virus for Linux 環境設定ガイド」に説明のある savconfig コマンドおよび savscan コマンドを使用して設定を変更することができます。

UNIX コンピュータでは、「Sophos Anti-Virus for UNIX 環境設定ガイド」に説明のある savscan コマンドを使用して設定を変更することができます。

検索の対象から除外できる項目

コンピュータの種類によって、検索の対象から除外できる項目は異なります。

Windows

Windows 環境では、ドライブ、フォルダ、ファイルおよびプロセスを除外できます。

ワイルドカード文字「*」、および「?」を使用できます。

ワイルドカード文字「?」は、ファイル名や拡張子の指定のみに使用できます。通常、任意の 1 文字を表します。しかし、ファイル名や拡張子の末尾に使用した場合は、任意の 1文字、または文字のない状態と一致します。たとえば、「file??.txt」は、「file.txt」や「file1.txt」、および「file12.txt」に一致しますが、「file123.txt」には一致しません。

ワイルドカード文字「*」は、ファイル名や拡張子に対して、[ファイル名].*、または *.[拡張子] という形式だけで使用できます。つまり、「file*.txt」、「file.txt*」、および「file.*txt」などは無効です。

Mac OS X

Mac OS X 環境では、ファイル、フォルダ、およびボリュームを除外できます。

除外項目の前や末尾に「/」を付け加えたり、除外項目の末尾に「//」を付け加えたりすることにより、除外する項目を指定できます。

詳細は、Sophos Anti-Virus for Mac OS X ヘルプを参照してください。

Linux または UNIX

Linux や UNIX では、ディレクトリやファイルを除外できます。

ファイルやディレクトリであるかに関わらず、POSIX パスを指定できます。例: /フォルダ名/ファイル名。ワイルドカード文字「?」および「*」が使用できます。

注
Enterprise Console では、Linux および UNIX コンピュータに対しては、パスの指定による方法のみで除外を設定できます。他のタイプの除外は、直接、管理対象コンピュータから設定できます。この場合、正規表現を使用したり、ファイルの種類やファイルシステムを除外できます。操作方法の詳細は、「Sophos Anti-Virus for Linux 環境設定ガイド 」または「Sophos Anti-Virus for UNIX 環境設定ガイド」を参照してください。

管理対象の Linux または UNIX コンピュータで、パスの指定による別の除外を設定した場合、そのコンピュータはグループポリシーと異なるコンピュータとしてコンソール画面にレポートされます。

検索の対象から項目を除外する方法の詳細は、次のトピックを参照してください。

- オンアクセス検索の対象から項目を除外する (p. 87)
- オンデマンド検索やスケジュール検索の対象から項目を除外する (p. 94)

Windows での検索の除外を指定する

標準的な命名規則

Sophos Anti-Virus で、ファイル名やパスは、標準的な命名規則に照合して認証されます。たとえば、フォルダ名にスペース文字を含めることはできますが、スペース文字のみで構成することはできません。

二重拡張子

二重拡張子を持つファイル名は、最終拡張子のみ拡張子として扱われ、それ以外の拡張子はファイル名の一部として扱われます。

MySample.txt.doc = ファイル名 [MySample.txt] + 拡張子 [.doc]

特定のファイル、フォルダ、ドライブの除外

除外の種類	説明	例	コメント
特定のファイル	特定のファイルを除外するには、パスとファイル名の両方を指定します。パスには、ドライブ文字やネットワークの共有フォルダ名を含めることができます。	C:¥Documents ¥CV.doc ¥¥Server¥Users ¥Documents ¥CV.doc	除外が常に正しく適用されるようにするには、ファイル名やフォルダ名を長い名前と短い名前 (8.3 形式) の両方の形式で指定してください。 C:¥Program Files¥Sophos ¥Sophos Anti-Virus C: ¥Progra~1¥Sophos ¥Sophos~1 詳細は、サポートデータベースの文章 13045 を参照してください。
特定のファイル名のファイルすべて	ファイルシステム上にある特定のファイル名のファイルすべてを除外するには、パスなしでファイル名を指定します。	spacer.gif	
特定のドライブやネットワーク共有フォルダ内のアイテムすべて	特定のドライブやネットワーク共有フォルダ内のアイテムすべてを除外するには、ドライブ文字やネットワークの共有フォルダ名を指定します。	D: ¥¥サーバー名 ¥<共有名>¥	ネットワーク共有を指定する場合は、共有名の後にバックスラッシュを付けます。
特定のフォルダ	特定のフォルダとそのサブフォルダ内のアイテムすべてを除外するには、ドライブ文字やネットワーク共有フォルダ名を使用してフォルダパスを指定します。	D:¥Tools¥logs¥	フォルダ名の後にバックスラッシュを入力します。

除外の種類	説明	例	コメント
特定のフォルダ名のフォルダすべて	**すべて**のドライブやネットワーク共有フォルダにある、特定のフォルダとそのサブフォルダ内のアイテムすべてを除外するには、ドライブ文字やネットワーク共有フォルダ名を使用せずにフォルダパスを指定します。	¥Tools¥logs¥ (次のフォルダが除外されます。C:¥Tools¥logs¥、¥¥Server¥Tools¥logs¥)	ドライブ文字やネットワーク共有フォルダ名直前までのパスすべてを指定する必要があります。この例で、¥logs¥ と指定しても何も除外されません。

ワイルドカード文字

ワイルドカード文字「?」、および「*」を使用できます。

ファイル名や拡張子で任意の 1文字を指定するには、ワイルドカード文字「?」を使用します。

ファイル名や拡張子の末尾に使用した場合は、任意の 1文字、または文字のない状態と一致します。たとえば、「file??.txt」は、「file.txt」や「file1.txt」、および「file12.txt」に一致しますが、「file123.txt」には一致しません。

ワイルドカード文字「*」は、ファイル名や拡張子に対して、[ファイル名].*、または *.[拡張子] という形式で使用します。

正:

file.*

*.txt

誤:

file.txt*

file.*txt

特定の文字ではじまる、特定の拡張子のあるファイルを除外することもできます。

file*.txt

上のように指定すると、次のようなファイルが検索から除外されます。

file.txt

file1.txt

file12.txt

file.1.txt

file.12.txt

file12.12.txt

なお、上のように指定しても、次のようなファイルは除外されません。

file.1txt

file.12txt

file.txt1

file.txt12

1file.txt

1file.txt1

7.1.8 使用するアイテムを認証する

アドウェアや不要と思われるアプリケーションを認証する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Sophos Endpoint Security and Control で、アドウェアや他の不要と思われるアプリケーション (PUA) の検出を有効にした場合、必要なアプリケーションの使用がブロックされることがあります。

アドウェアや不要と思われるアプリケーションを認証する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**認証**」をクリックします。
   「**認証マネージャ**」ダイアログボックスが表示されます。
5. 「**アドウェアや不要と思われるアプリケーション**」タブで、「**既知アドウェアや不要と思われるアプリケーション**」リストから、認証するアプリケーションを選択します。
   認証するアプリケーションが表示されない場合は、既知アドウェアや不要と思われるアプリケーションのリストに手動で追加することができます。操作方法の詳細は、アドウェアや不要と思われるアプリケーションを事前に認証する (p. 109) を参照してください。
6. 「**追加**」をクリックします。

追加したアドウェアや不要と思われるアプリケーションは、「**認証済みアドウェアや不要と思われるアプリケーション**」リストに表示されます。

アドウェアや不要と思われるアプリケーションを事前に認証する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Sophos Endpoint Security and Control でアドウェアや不要と思われるアプリケーションとして分類されていないアプリケーションの使用を許可するには、そのアプリケーションを、認証済みア

ドウェア/不要と思われるアプリケーションのリストに手動で追加することにより、事前に認証することができます。

1. ソフォス Web サイトの**アドウェアと不要なアプリケーション**ページ (http://www.sophos.com/ja-jp/threat-center/threat-analyses/adware-and-puas.aspx) を開きます。
2. 事前に認証するアプリケーションの名前を検索し、コピーします。
3. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
4. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
5. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
6. 「**認証**」をクリックします。
   「**認証マネージャ**」ダイアログボックスが表示されます。
7. 「**アドウェアや不要と思われるアプリケーション**」タブで、「**新規エントリ**」をクリックします。
8. 「**アドウェアや不要と思われるアプリケーションの追加**」ダイアログボックスに、ステップ 2 でコピーしたアプリケーション名を貼り付けます。

追加したアドウェアや不要と思われるアプリケーションは、「**認証済みアドウェアや不要と思われるアプリケーション**」リストに表示されます。

操作を誤った場合や、「**認証マネージャ**」からアプリケーションを削除したい場合は、既知アドウェアや不要と思われるアプリケーションのリストから削除できます。

1. 「**認証済みアドウェアや不要と思われるアプリケーション**」リストで、削除するアプリケーションを選択します。
2. 「**削除**」をクリックします。
3. 「**既知アドウェアや不要と思われるアプリケーション**」リストで、削除するアプリケーションを選択します。
4. 「**エントリの削除**」をクリックします。

認証済みアドウェアや不要と思われるアプリケーションをブロックする

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

一度認証したアドウェアや不要と思われるアプリケーションの実行をブロックする方法は次のとおりです。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**ウイルス対策および HIPS ポリシー**」ダイアログボックスで、「**認証**」ボタンをクリックします。

4. 「**アドウェアや不要と思われるアプリケーション**」タブで、「**認証済みアドウェアや不要と思われるアプリケーション**」リストから、ブロックするアプリケーションを選択します。
5. 「**削除**」をクリックします。

疑わしいアイテムを認証する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1つ以上の HIPS オプション (疑わしい動作の検知、バッファオーバーフローの検知、または疑わしいファイルの検出など) を有効にしており、必要なアイテムが検出された場合、次のようにアイテムを認証すると使用できるようになります。

1. 設定するコンピュータのグループ (複数可) に、どのウイルス対策および HIPS ポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**認証**」をクリックします。
   「**認証マネージャ**」ダイアログボックスが表示されます。
5. 検出された動作の種類に対応するタブをクリックします。
   この例では、「**バッファオーバーフロー**」を使用します。
6. 「**既知アプリケーション**」リストで、認証するアプリケーションを選択します。
   認証するアプリケーションが表示されない場合は、認証済みアプリケーションのリストに手動で追加できます。操作方法の詳細は、アドウェアや不要と思われるアプリケーションを事前に認証する (p. 109) を参照してください。
7. 「**追加**」をクリックします。

疑わしいアプリケーションが「**認証済みアプリケーション**」のリストに表示されます。

疑わしいと思われるアイテムを事前に認証する

Sophos Endpoint Security and Control で疑わしいと思われるアイテムとして分類されていないアプリケーションやファイルの使用を許可するには、そのアプリケーションやファイルを、認証済みアイテムのリストに手動で追加することにより、事前に認証することができます。

1. 設定するコンピュータのグループ (複数可) に、どのウイルス対策および HIPS ポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**認証**」をクリックします。
   「**認証マネージャ**」ダイアログボックスが表示されます。
5. 検出された動作の種類に対応するタブをクリックします。
   この例では、「**バッファオーバーフロー**」を使用します。

6. 「**新規エントリ**」をクリックします。
   「**ファイルを開く**」ダイアログボックスが表示されます。
7. アプリケーションを参照し、それをダブルクリックします。

疑わしいアプリケーションが「**認証済みアプリケーション**」のリストに表示されます。

操作を誤った場合や、「**認証マネージャ**」からアプリケーションを削除したい場合は、既知ファイルのリストから削除できます。

1. 「**認証マネージャ**」ダイアログボックスで、検出された動作の種類に対応するタブをクリックします。

   この例では、「**疑わしいファイル**」を使用します。
2. 「**認証済みファイル**」リストで、ファイルを選択します。
3. 「**削除**」をクリックします。
4. 「**既知ファイル**」リストで、ファイルを選択します。
5. 「**エントリの削除**」をクリックします。

Web サイトを認証する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ソフォス製品で悪意のあるサイトとして分類される Web サイトを認証するには、対象のサイトを認証するサイトへ追加します。Web サイトを認証すると、認証した Web サイトの URL はソフォスのオンライン Web フィルタリングサービスで検証されなくなります。

注意
ソフォス製品で悪意のあるサイトとして分類されている Web サイトを認証すると、ユーザーのコンピュータが脅威に感染する可能性が高くなります。このため、サイトを認証する前に、閲覧しても安全であることを必ず確認してください。

Web サイトを認証する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのウイルス対策および HIPS ポリシーが指定されているかを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ウイルス対策および HIPS**」をダブルクリックします。
3. 変更するポリシーをダブルクリックします。
   「**ウイルス対策および HIPS ポリシー**」ダイアログボックスが表示されます。
4. 「**認証**」をクリックします。
   「**認証マネージャ**」ダイアログボックスが表示されます。
5. 「**Web サイト**」タブで、「**追加**」をクリックします。
   - Web サイトを編集するには、「**認証済み Web サイト**」の一覧で Web サイトを選択して、「**編集**」をクリックします。
   - Web サイトを削除するには、「**認証済み Web サイト**」 の一覧で Web サイトを選択して、「**削除**」をクリックします。

「**認証済み Web サイト**」の一覧に、追加した Web サイトが表示されます。

注

- ダウンロードスキャンを有効にしている場合、脅威を含む Web サイトにユーザーがアクセスすると、認証済み Web サイトに指定されていても同サイトへのアクセスはブロックされます。
- Web コントロール機能を使用している場合、既に **Web コントロール** ポリシーでブロック済みの Web サイトを、ここでの操作で認証してもアクセスできるようにはなりません。アクセスを許可するには、ウイルス対策および HIPS ポリシーで認証するだけでなく、Web コントロール機能で、例外 Web サイトに指定し、許可する必要があります。Web コントロールの詳細は、Web コントロール ポリシー (p. 177)を参照してください。

7.2 ファイアウォール ポリシー

ファイアウォールポリシーでは、ファイアウォールによってコンピュータがどのように保護されるかを設定します。

デフォルトで、Sophos Client Firewall は有効に設定され、必須のトラフィック以外はすべてブロックされます。ネットワーク全体でファイアウォールを使用する前に、必要なアプリケーションの使用を許可するようファイアウォールを設定してください。詳細は、基本的なファイアウォールポリシーを設定する (p. 113)を参照してください。

デフォルトのファイアウォール設定について、詳細はサポートデータベースの文章 57757 を参照してください。

注
Windows 8 以降対応版の Sophos Client Firewall 3.0 では、複数の機能が廃止されています。これらの機能は、Windows 7 以前が稼動しているコンピュータのみで利用できます。削除された機能は以下のとおりです。

- 対話型モード
- 隠しプロセス検知
- メモリの変更検知
- RAW ソケット アプリケーション (RAW ソケットは他の接続と同様に処理されます)
- 非ステートフル ルール
- TCP ルールに対する**コンカレント接続**オプション
- **ローカルポートがリモートポートと同じ場合**オプション

7.2.1 ファイアウォールの基本設定

基本的なファイアウォールポリシーを設定する

デフォルトで、ファイアウォールは有効に設定されるため、必須のトラフィック以外はすべてブロックされます。したがって、必要なアプリケーションが許可されるよう設定し、テストを行ってから、ネットワーク上のすべてのコンピュータにインストールしてください。詳細は「Sophos Enterprise Console ポリシー設定ガイド」を参照してください。

デフォルトのファイアウォール設定について、詳細はソフォスのサポートデータベースの文章 57757 を参照してください。

ネットワークのブリッジ接続の防止について、詳細はデバイスコントロール ポリシー (p. 164)を参照してください。

重要
新しいポリシーや、更新したポリシーをコンピュータに適用すると、新しいポリシーが完全に適用されるまでの短い間、適用前に起動が許可されていたアプリケーションがブロックされることがあります。新しいポリシーを適用する際は、前もってその旨をユーザーに通知してください。

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

基本的なファイアウォールポリシーを設定する方法は次のとおりです。

1. 「**ポリシー**」ペインで、「**ファイアウォール**」をダブルクリックします。
2. 「**デフォルト**」ポリシーをダブルクリックして編集します。
「**ファイアウォール ポリシー**」ウィザードが表示されます。画面の指示に従います。一部のオプションについての追加情報は以下のとおりです。
3. 「**ファイアウォールの環境設定**」ページで、接続先の種類を設定します。
   - デスクトップなど、常に社内ネットワークに接続されているコンピュータに対しては、「**1種類の設定 (固定マシン用)**」を選択します。
   - 社内ネットワークや社外など、コンピュータを使う場所に応じて、異なるファイアウォールの設定を使い分ける場合は、「**2種類の設定 (モバイル PC 用)**」を選択します。「2種類の設定 (モバイル PC 用)」は、モバイル PC に適しています。
4. 「**操作モード**」ページで、ファイアウォールが送受信トラフィックを処理する方法を選択します。

モード	説明
送受信トラフィックをブロックする	• デフォルト設定。最高レベルのセキュリティを提供します。 • 必要なトラフィックのみを許可し、チェックサムを使用してアプリケーションの認証を行います。 • 組織内でよく使うアプリケーションに対して、ファイアウォール経由での接続を許可するには、「**信頼**」ボタンをクリックします。詳細は、アプリケーションの信頼について (p. 122)を参照してください。
受信トラフィックをブロックし、送信トラフィックを許可する	• 「**送受信トラフィックをブロックする**」モードよりも低いセキュリティレベルを提供します。 • 特定のルールを作成することなく、ご使用のコンピュータは、ネットワークとインターネットにアクセスできます。

モード	説明
	• すべてのアプリケーションは、ファイアウォール経由での接続が許可されています。
監視する	• 設定したルールをネットワークトラフィックに適用します。一致するルールのないトラフィックは、管理コンソールにレポートされ、送信方向の場合のみ許可されます。 • ネットワーク情報を収集し、各コンピュータにファイアウォールをインストールする前に、集めた情報に基づいて適切なルールを作成できます。詳細は、監視モードの使用について (p. 115)を参照してください。

5. コンピュータ間のプリンタやフォルダの共有を許可する場合は、「**ファイルとプリンタの共有**」ページで、「**ファイルとプリンタの共有を許可する**」を選択します。

ファイアウォールの設定を完了すると、「**ファイアウォール - イベントビューア**」で、ファイアウォールでブロックされたアプリケーションなど、ファイアウォールのイベントを表示できます。詳細は、ファイアウォールのイベントを表示する (p. 201)を参照してください。

また、過去 1週間で、しきい値を超える数のイベントが発生したコンピュータの台数がダッシュボードに表示されます。

監視モードの使用について

テスト用コンピュータで監視モードを有効にして、「ファイアウォール - イベントビューア」を使って、使用されているトラフィック、アプリケーション、およびプロセスを表示できます。

表示されるトラフィック、アプリケーションおよびプロセスを許可/ブロックするルールは、イベントビューアで簡単に作成できます。詳細は、ファイアウォールのイベントのルールを作成する (p. 119)を参照してください。

注
「ファイアウォール - イベントビューア」を使って、ルールを作成し、ファイアウォールポリシーに追加する際は、ファイアウォールの操作モードが「**監視**」から「**カスタム**」に変わります。

デフォルトで不明なトラフィックを許可しないようにする場合は、対話型モードを利用できます。

対話型モードでは、ルールが指定されていないアプリケーションやトラフィックに対して、許可/ブロックするかを選択するようメッセージが表示されます。詳細は、対話型モード (p. 121)を参照してください。

信頼するアプリケーションを追加する

信頼できるアプリケーションには、インターネットを含む、ネットワークへのフルアクセスが無条件に許可されています。

ファイアウォールポリシーに信頼するアプリケーションを追加する方法は次のとおりです。

1. 「**ファイアウォール ポリシー**」ウィザードの「**操作モード**」ページで、「**信頼**」をクリックします。

「**ファイアウォール ポリシー**」ダイアログボックスが表示されます。

2. 「**追加**」をクリックします。
   「**ファイアウォール ポリシー - 信頼できるアプリケーションの追加**」ダイアログボックスが表示されます。
3. 「**検索期間**」フィールドで、ドロップダウン矢印をクリックし、アプリケーションのイベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
4. 特定の種類のアプリケーションのイベントを表示するには、「**イベントタイプ**」フィールドで、ドロップダウン矢印をクリックし、イベントの種類を選択します。
5. 特定のファイルに関するアプリケーションのイベントを表示するには、「**ファイル名**」フィールドにファイル名を入力します。
   フィールドを空欄のままにすると、すべてのファイルに関するアプリケーションのイベントが表示されます。
   このフィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
6. 「**検索**」をクリックし、アプリケーションのイベントの一覧を表示します。
7. アプリケーションのイベントを選択し、「**OK**」をクリックします。

「**信頼する**」アプリケーションとして、ファイアウォール ポリシーにアプリケーションが追加されます。

ロールベースの管理

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

LAN 上のトラフィックすべてを許可する

LAN (ローカル エリア ネットワーク) 上のコンピュータ間のトラフィックすべてを許可する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのファイアウォールポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ファイアウォール**」をダブルクリックし、変更するポリシーをダブルクリックします。
3. 「**ファイアウォールポリシー**」ウィザードの「**ファイルとプリンタの共有**」ページで、「**カスタム設定を使用する**」を選択し、「**カスタム**」をクリックします。
4. 「**LAN の設定**」リストで、ネットワークに対して、「**信頼**」チェックボックスを選択します。

注
LAN 上のコンピュータ間のトラフィックすべてを許可すると、ファイルとプリンタの共有も許可することになります。

ロールベースの管理

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ファイルとプリンタの共有を許可する

コンピュータ間のプリンタやフォルダの共有を許可する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのファイアウォールポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ファイアウォール**」をダブルクリックし、変更するポリシーをダブルクリックします。
3. 「**ファイアウォールポリシー**」ウィザードの「**ファイルとプリンタの共有**」ページで、「**ファイルとプリンタの共有を許可する**」を選択します。

ロールベースの管理

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ファイルとプリンタの共有の許可を詳細に設定する

社内ネットワーク上のファイルとプリンタの共有を詳細に設定する (片方向の NetBIOS トラフィックなど) には、次のようにします。

- 「**LAN の設定**」リストに記載されていない LAN (ローカルエリアネットワーク) に対してファイルとプリンタの共有を許可します。これにより、このような LAN 上の NetBIOS トラフィックがファイアウォールのルールで処理されるようになります。
- 適切な NetBIOS ポートやプロトコルの場合、ホストとの双方向の通信を許可する設定で優先度の高いルールを作成します。不要なファイルとプリンタの共有トラフィックは、デフォルトのルールで処理するのではなく、すべて明示的にブロックすることを推奨します。

「**LAN の設定**」リストに記載されていない LAN (ローカルエリアネットワーク) LAN に対してファイルとプリンタの共有を許可する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのファイアウォールポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。

2. 「**ポリシー**」ペインで、「**ファイアウォール**」をダブルクリックし、変更するポリシーをダブルクリックします。
3. 「**ファイアウォールポリシー**」ウィザードの「**ファイルとプリンタの共有**」ページで、「**カスタム設定を使用する**」を選択し、「**カスタム**」をクリックします。
4. 「**他のネットワークに対するファイルとプリンタの共有をブロックする**」チェックボックスの選択を外します。

ロールベースの管理

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

不要なファイルとプリンタの共有をブロックする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「**LAN の設定**」リストに記載されていない LAN 上のファイルとプリンタの共有をブロックするには、「**LAN**」タブで次の操作を行います。

1. 設定するコンピュータのグループに、どのファイアウォールポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ファイアウォール**」をダブルクリックし、変更するポリシーをダブルクリックします。
3. 「**ファイアウォールポリシー**」ウィザードの「**ファイルとプリンタの共有**」ページで、「**カスタム設定を使用する**」を選択し、「**カスタム**」をクリックします。
4. 「**他のネットワークに対するファイルとプリンタの共有をブロックする**」チェックボックスを選択します。

ファイアウォールのイベントのルールを作成する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「変更されたメモリ」以外のすべてのファイアウォールイベントに対してルールを作成できます。

ファイアウォールのイベントのルールを作成する方法は次のとおりです。

1. 「**イベント**」メニューの「**ファイアウォールのイベント**」をクリックします。
2. 「**ファイアウォール - イベントビューア**」ダイアログボックスで、ルールを作成するアプリケーションのイベントを選択し、「**ルールの作成**」をクリックします。
3. 表示されるダイアログボックスで、アプリケーションに適用するオプションを選択します。
4. ルールを適用するロケーション (プライマリ、セカンダリ、またはその両方) を選択します。ルールの適用先をセカンダリロケーションまたは両方のロケーションにした場合は、セカンダリロケーションが設定されているポリシーのみにルールが追加されます。「**OK**」をクリックします。

   注
   「新規アプリケーション」と「変更されたアプリケーション」イベントは、両方のロケーションが共有するチェックサムを追加するため、どちらかのロケーションに依存するものではありません。このため、これらのイベントに対してロケーションを選択することはできません。

5. ファイアウォールポリシーの一覧から、ルールを適用するポリシー (複数可) を選択します。「**OK**」をクリックします。

   注
   各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーにだけルールを追加できます。

注
「ファイアウォールの詳細ポリシー」の設定ページで、ファイアウォールポリシーから直接アプリケーション ルールを作成する場合は、ファイアウォールポリシーからアプリケーションルールを作成する (p. 137)を参照してください。

ファイアウォールを一時的に無効にする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、ファイアウォールは有効になっています。しかし、保守作業やトラブルシューティングのために、ファイアウォールを一時的に無効化し、有効に戻さなければならないこともあります。

各コンピュータのグループに対して、ファイアウォールを無効にする方法は次のとおりです。

1. 設定するコンピュータのグループに、どのファイアウォールポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ファイアウォール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
   「**ファイアウォール ポリシー**」ウィザードが表示されます。
3. ウィザードの「ようこそ」ページで、次のいずれかを実行します。
   - 設定したすべてのロケーション (プライマリロケーション、および設定した場合はセカンダリロケーション) でファイアウォールを無効にする場合は、「**次へ**」をクリックします。「**ファイアウォールの環境設定**」ページで、「**すべてのトラフィックを許可する (ファイアウォールを無効にする)**」を選択します。ウィザードを完了します。
   - いずれかのロケーション (プライマリ、またはセカンダリ) でファイアウォールを無効にする場合は、「**ファイアウォールの詳細ポリシー**」ボタンをクリックします。表示される「**ファイアウォール ポリシー**」ダイアログボックスで、「**プライマリロケーション**」または「**セカンダリロケーション**」の横にある「**すべてのトラフィックを許可する**」を選択します。「**OK**」をクリックします。「**ファイアウォール ポリシー**」ウィザードを完了してください。

ファイアウォールを無効にすると、再度有効にするまでコンピュータは保護されません。ファイアウォールを有効にするには、「**すべてのトラフィックを許可する**」チェックボックスを選択から外します。

7.2.2 ファイアウォールの詳細設定

詳細設定ページを開く

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

より柔軟かつ詳細にファイアウォールを設定するには、「ファイアウォールの詳細ポリシー」の設定ページを使います。

ファイアウォールの詳細設定ページを開く方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。

対話型モード

対話モードは、Windows 7 以前を実行しているコンピュータで使用できます。対話型モードでは、登録されていないアプリケーションやサービスがネットワークアクセスを要求するたびに、エンドポイントコンピュータにファイアウォールの対話型ダイアログが表示されます。対話型ダイアログには、トラフィックを許可する、トラフィックをブロックする、あるいはそのタイプのトラフィックを処理する共通ルールを作成するといった内容の選択肢が表示されます。

注
Windows 8 以降では、対話型モードは使用できません。特定のポリシールールを追加して、アプリケーションを許可/ブロックする必要があります。「**ファイアウォール - イベントビューア**」を利用すれば、対話型モードと同じ要領でアプリケーションのルールを作成することができます。詳細は、ファイアウォールのイベントのルールを作成する (p. 119)を参照してください。

対話型モードを有効にする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ファイアウォールを対話型モードに設定すると、検出したトラフィックの処理方法について、ユーザーに確認するメッセージが表示されます。詳細は、対話型モード (p. 121)を参照してください。

各コンピュータのグループに対して、ファイアウォールを対話型モードに切り替える方法は次のとおりです。

1. 設定するコンピュータのグループに、どのファイアウォールポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するロケーション用の「**環境設定**」をクリックします。
4. 「**全般**」タブの「**動作モード**」パネルで、「**対話型**」をクリックします。

非対話型モードに変更する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

非対話型モードには次の 2とおりがあります。

- 規定で許可
- 規定でブロック

ファイアウォールの非対話型モードでは、指定されているルールでネットワークトラフィックが自動的に処理されます。ルールと一致しないネットワークトラフィックは、すべて許可 (送信方向の場合)、またはすべてブロックされます。

各コンピュータのグループに対して、ファイアウォールを非対話型モードに切り替える方法は次のとおりです。

1. 「**ポリシー**」ペインで、「**ファイアウォール**」をダブルクリックし、変更するポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するロケーション用の「**環境設定**」をクリックします。
4. 「**全般**」タブをクリックします。
5. 「**動作モード**」パネルで、「**規定で許可**」または「**規定でブロック**」をクリックします。

ファイアウォールを設定する

アプリケーションの信頼について

ファイアウォールは、認証されていないアプリケーションのトラフィックをブロックし、コンピュータを守ります。しかし、社内でよく使われるアプリケーションがブロックされ、日常業務に支障をきたすこともあります。

このようなアプリケーションは信頼することで、ファイアウォール経由での接続が可能になります。信頼できるアプリケーションには、ネットワークおよびインターネットへのフルアクセスが無条件に許可されています。

注
より安全を期すには、アプリケーションのルールを適用して (複数可)、アプリケーションの実行を許可する条件を指定できます。操作方法の詳細は、ファイアウォールポリシーからアプリケーション ルールを作成する (p. 137) を参照してください。

ファイアウォール ポリシーにアプリケーションを追加する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ファイアウォール ポリシーにアプリケーションを追加する方法は次のとおりです。

1. 「**環境設定**」パネルで、設定するロケーション用の「**環境設定**」をクリックします。
2. 「**アプリケーション**」タブをクリックします。
3. 「**追加**」をクリックします。
   「**ファイアウォール ポリシー - アプリケーションの追加**」ダイアログボックスが表示されます。
4. 「**検索期間**」フィールドで、ドロップダウン矢印をクリックし、アプリケーションのイベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
5. 特定の種類のアプリケーションのイベントを表示するには、「**イベントタイプ**」フィールドで、ドロップダウン矢印をクリックし、イベントの種類を選択します。
6. 特定のファイルに関するアプリケーションのイベントを表示するには、「**ファイル名**」フィールドにファイル名を入力します。
   フィールドを空欄のままにすると、すべてのファイルに関するアプリケーションのイベントが表示されます。
   このフィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
7. 「**検索**」をクリックし、アプリケーションのイベントの一覧を表示します。
8. アプリケーションのイベントを選択し、「**OK**」をクリックします。

- 「**信頼する**」アプリケーションとして、ファイアウォール ポリシーにアプリケーションが追加されます。
- このアプリケーションのチェックサムが許可するチェックサムのリストに追加されます。

ファイアウォールポリシーからアプリケーションを削除する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ファイアウォールポリシーからアプリケーションを削除する方法は次のとおりです。

1. 「**環境設定**」パネルで、設定するロケーション用の「**環境設定**」をクリックします。
2. 「**アプリケーション**」タブをクリックします。
3. リストに表示されるアプリケーションを選択し、「**削除**」をクリックします。

アプリケーションを信頼する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

グループ内のコンピュータのアプリケーションを信頼する方法は次のとおりです。

1. 「**環境設定**」パネルで、設定するロケーション用の「**環境設定**」をクリックします。
2. 「**アプリケーション**」タブをクリックします。
   アプリケーションがリストにない場合は、ファイアウォール ポリシーにアプリケーションを追加する (p. 123)の手順に従って追加します。
3. リストに表示されるアプリケーションを選択し、「**信頼**」をクリックします。

- 「**信頼する**」アプリケーションとして、ファイアウォール ポリシーにアプリケーションが追加されます。
- このアプリケーションのチェックサムが許可するチェックサムのリストに追加されます。

信頼できるアプリケーションには、インターネットを含む、ネットワークへのフルアクセスが無条件に許可されています。より安全を期すには、アプリケーションのルールを適用して (複数可)、アプリケーションの実行を許可する条件を指定できます。

- アプリケーション ルールを作成する (p. 136)
- アプリケーションにプリセットルールを適用する (p. 139)

ファイアウォール イベント ビューアを使用して信頼するアプリケーションを登録する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ファイアウォールが不明なアプリケーションを検知したり、ネットワーク上のコンピュータのアプリケーションをブロックすると、「ファイアウォール - イベントビューア」にイベントが表示されます。このトピックでは、「ファイアウォール - イベントビューア」から信頼するアプリケーションを登録する方法や、任意のファイアウォール ポリシーに新しいルールを適用する方法について説明します。

「ファイアウォール - イベントビューア」で、検知またはブロックされたアプリケーションの詳細を表示し、それらのアプリケーションを信頼するアプリケーションとして登録する方法、および新しいルールを作成する方法は次のとおりです。

1. 「**イベント**」メニューの「**ファイアウォールのイベント**」をクリックします。
2. 「**ファイアウォール - イベントビューア**」ダイアログボックスで、信頼する、または新しいルールを作成するアプリケーションのエントリを選択し、「**ルールの作成**」をクリックします。
3. 表示されるダイアログボックスで、アプリケーションを信頼するか、または既存のプリセットルールを使って、アプリケーションに対してルールを作成するかを選択します。
4. ファイアウォールポリシーの一覧から、ルールを適用するファイアウォールポリシーを選択します。すべてのファイアウォールにルールを適用するには、「**すべてを選択**」をクリックして「**OK**」をクリックします。

- チェックサムを使用している場合は、許可されているチェックサムの一覧へのアプリケーションのチェックサムの追加が必要になることがあります。詳細は、アプリケーションのチェックサムを追加する (p. 128)を参照してください。
- また、「ファイアウォールの詳細ポリシー」の設定ページで、信頼するアプリケーションを直接ファイアウォールポリシーに追加することもできます。詳細は、ファイアウォールポリシーからアプリケーション ルールを作成する (p. 137)を参照してください。

アプリケーションをブロックする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

グループ内のコンピュータのアプリケーションをブロックする方法は次のとおりです。

1. 設定するコンピュータのグループに、どのファイアウォールポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ファイアウォール**」をダブルクリックし、変更するポリシーをダブルクリックします。

3. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
4. 「**環境設定**」パネルで、設定するロケーション用の「**環境設定**」をクリックします。
5. 「**アプリケーション**」タブをクリックします。
   アプリケーションがリストにない場合は、ファイアウォール ポリシーにアプリケーションを追加する (p. 123)の手順に従って追加します。
6. リストに表示されるアプリケーションを選択し、「**ブロック**」をクリックします。

アプリケーションが隠しプロセスを起動することを許可する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

アプリケーションは、ネットワークにアクセスするため、別の隠しプロセスを起動することがあります。

悪意のあるアプリケーションは、この手法を利用してファイアウォールを迂回することがあります。つまり、自身ではなく信頼できるアプリケーションを起動してネットワークに接続します。

アプリケーションに対して隠しプロセスの起動を許可するには、次の手順を実行してください。

注
Windows 8 以降の環境では、Sophos Anti-Virus の HIPS テクノロジーによって自動処理されるため、このオプションを使用することはできません。

1. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
2. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
3. 「**プロセス**」タブをクリックします。
4. ダイアログボックスの上部で、「**追加**」をクリックします。
   「**ファイアウォール ポリシー - アプリケーションの追加**」ダイアログボックスが表示されます。
5. 「**検索期間**」フィールドで、ドロップダウン矢印をクリックし、アプリケーションのイベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
6. 特定のファイルに関するアプリケーションのイベントを表示するには、「**ファイル名**」フィールドにファイル名を入力します。
   フィールドを空欄のままにすると、すべてのファイルに関するアプリケーションのイベントが表示されます。
   このフィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
7. 「**検索**」をクリックし、アプリケーションのイベントの一覧を表示します。
8. アプリケーションのイベントを選択し、「**OK**」をクリックします。

ファイアウォールの対話型モードを有効にしている場合、新たなランチャが検出された際に、エンドポイントコンピュータ上に対話型ダイアログを表示することができます。詳細は、対話型モードを有

効にする (p. 121)を参照してください。Windows 8 以降の環境で対話型モードを使用することはできません。

アプリケーションが RAW ソケットを使用することを許可する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

アプリケーションのなかには、RAW ソケットを使用してネットワークにアクセスできるものもあります。RAW ソケットを使用すると、ネットワークを介して送信するデータのあらゆる点を制御することができます。

悪意のあるアプリケーションは、IP アドレスを偽ったり、破損したメッセージを故意に送信するなど、RAW ソケットを悪用することができます。

アプリケーションに対して RAW ソケットを使用したネットワークへのアクセスを許可するには、次の手順を実行してください。

注
Windows 8 以降の環境でこのオプションを使用することはできません。ファイアウォールは、通常のソケットと同様に RAW ソケットを処理します。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**プロセス**」タブをクリックします。
5. ダイアログボックスの下部で、「**追加**」をクリックします。
   「**ファイアウォール ポリシー - アプリケーションの追加**」ダイアログボックスが表示されます。
6. 「**検索期間**」フィールドで、ドロップダウン矢印をクリックし、アプリケーションのイベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
7. 特定のファイルに関するアプリケーションのイベントを表示するには、「**ファイル名**」フィールドにファイル名を入力します。
   フィールドを空欄のままにすると、すべてのファイルに関するアプリケーションのイベントが表示されます。
   このフィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
8. 「**検索**」をクリックし、アプリケーションのイベントの一覧を表示します。
9. アプリケーションのイベントを選択し、「**OK**」をクリックします。

ファイアウォールの対話型モードを有効にしている場合、RAW ソケットが検出された際に、エンドポイントコンピュータ上に対話型ダイアログを表示することができます。詳細は、対話型モードを有効にする (p. 121)を参照してください。

アプリケーションのチェックサムを追加する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

各アプリケーションがバージョンごとに持つ固有のチェックサム。ファイアウォールはこのチェックサムを使用して、アプリケーションが許可されているかどうかを判断できます。

デフォルトでファイアウォールは、実行される各アプリケーションのチェックサムを確認します。チェックサムが不明、または変更された場合、ファイアウォールは当該アプリケーションをブロックします。

許可されているアプリケーションのチェックサムのリストにチェックサムを追加する方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**チェックサム**」タブをクリックします。
4. 「**追加**」をクリックします。
   「**ファイアウォール ポリシー - アプリケーションチェックサムの追加**」ダイアログボックスが表示されます。
5. 「**検索期間**」フィールドで、ドロップダウン矢印をクリックし、アプリケーションのイベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
6. 「**イベントタイプ**」欄のドロップダウン矢印をクリックし、変更されたアプリケーションのチェックサムチェックサムを追加するか、または新しいアプリケーションを追加するかを選択します。
7. 特定のファイルに関するアプリケーションのイベントを表示するには、「**ファイル名**」フィールドにファイル名を入力します。
   フィールドを空欄のままにすると、すべてのファイルに関するアプリケーションのイベントが表示されます。
   このフィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
8. 「**検索**」をクリックし、アプリケーションのイベントの一覧を表示します。
9. チェックサムを追加するアプリケーションのイベントを選択し、「**OK**」をクリックします。

「**ファイアウォール ポリシー**」ダイアログボックスにある、許可されているアプリケーションのチェックサムのリストに、アプリケーションのチェックサムが追加されます。

ファイアウォールの対話型モードを有効にしている場合、新規または変更されたアプリケーションが検出された際に、エンドポイントコンピュータ上に対話型ダイアログを表示することができます。詳細は、対話型モードを有効にする (p. 121)を参照してください。

変更されたプロセスのブロックを有効/無効にする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

マルウェアは、ファイアウォールを迂回するため、信頼するプログラムが開始したメモリ内のプロセスを変更し、変更したプロセスを通じてネットワークに接続することがあります。

メモリで変更されたプロセスを検出し、ブロックするよう、ファイアウォールを設定することができます。

変更されたプロセスのブロックを有効/無効にする方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**全般**」タブの「**ブロック**」で、「**他のアプリケーションによるメモリの変更があった場合プロセスをブロックする**」チェックボックスを選択から外して、変更されたプロセスのブロックを無効にします。
   変更されたプロセスのブロックを有効にするには、チェクボックスを選択します。

メモリでプロセスに変更が加えられたことをファイアウォールが検出した場合、変更されたプロセスがネットワークにアクセスしないよう、ルールが追加されます。

注

- 変更されたプロセスのブロックは、常時無効に設定しておかないことを推奨します。必要な場合のみ無効にするようにしてください。
- 変更されたプロセスのブロックは、64ビット版の Windows や Windows 8 以降の環境には対応していません。Windows 8 以降の環境では、Sophos Anti-Virus の HIPS テクノロジーで自動処理されます。
- 変更されたプロセスのみがブロックされます。変更されたプログラムのネットワークアクセスはブロックされません。

チェックサムの使用を有効/無効にする

ファイアウォールでは、デフォルトでアプリケーションの認証にチェックサムが使用されます。アプリケーションを信頼するときや、ブロックするときに、アプリケーションはそのチェックサムによって自動的に識別されます (チェックサムは手動でも追加できます)。チェックサムに一致しないアプリケーションは、ブロックされます。

このオプションを無効にした場合、アプリケーションは、そのファイル名に基づいて識別されます。

チェックサムを使用したアプリケーションの認証を有効/無効にする方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。

3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**全般**」タブの「**ブロック**」で、「**チェックサムを使用してアプリケーションを認証する**」チェックボックスを選択するか、または選択を外します。

IPv6 パケットを許可/ブロックする

IPv6 パケットを許可/ブロックする方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**全般**」タブの「**ブロック**」で、「**IPv6 パケットをブロックする**」チェックボックスを選択するか、または選択を外します。

ICMP メッセージをフィルタリングする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ICMP (Internet Control Message Protocol) を使用して、ネットワーク上のコンピュータ間で、互いのエラーやステータス情報を共有することができます。送信または受信する ICMP メッセージを種類ごとに許可/ブロックすることができます。

ICMP メッセージのフィルタリングは、ネットワークプロトコルに関する知識がある場合のみ行ってください。各種 ICMP メッセージについての説明は、ICMP メッセージの種類の説明 (p. 130)を参照してください。

ICMP メッセージをフィルタリングする方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**ICMP**」タブで、特定のタイプの受信メッセージや送信メッセージを認証するには、それぞれ、「**In**」または「**Out**」チェックボックスを選択します。

ICMP メッセージの種類の説明

エコー要求、エコー応答	相手の応答や状態を確認するメッセージ。ホストは「**エコー要求**」を送信して、相手先からの「**エコー応答**」を待機します。通常 ping コマンドで実行することができます。
宛先に到達不能、エコー応答	IP データグラムを配信できない場合、ルーターから送信されるメッセージ。データグラムは、TCP/IP ネットワークで配信されるデータやパケットの単位です。
発信元の抑制	処理不能なスピードでデータを受信したときにホストまたはルーターから送信されるメッセージ。

	データグラムの転送スピードを遅くするよう送信元に要求するメッセージです。
リダイレクトメッセージ	別のルーターに送信されるべきデータグラムを受信したときにルーターから送信されるメッセージ。メッセージには、データグラムを以後送信する際に使用すべき正しい送信先アドレスが含まれます。ネットワークトラフィックの転送を最適化するために使用されます。
ルーター通知、ルーター選択	ホストにルーターの存在を通知するメッセージ。ルーターは、「**ルーター通知**」メッセージを定期的に送信して自身のアドレスをブロードキャストします。ホストが「**ルーター選択**」メッセージを送信してルーターのアドレスを要求する場合もあり、その場合、ルーターは、「**ルーター通知**」メッセージで応答します。
時間超過	データグラムがルーター通過用に設定されている時間を超えたときにルーターから送信されるメッセージ。
パラメータ問題	データグラムの送信中に問題が発生し、処理を終了できない場合にルーターから送信されるメッセージ。この問題の原因として、無効なデータグラムのヘッダなどがあります。
タイムスタンプ要求、タイムスタンプ応答	ホスト間の時刻同期を行い、転送時間を予測するために使用するメッセージ。
情報要求、情報応答	現在使用されていません。ホストのネットワークアドレスを検出するために使用されていましたが、現在では、古い機能とみなされているので使用しないでください。
アドレスマスク要求、アドレスマスク応答	サブネットのマスク (どのアドレスビットがネットワークアドレスを定義するのか) を検索するために使用するメッセージ。ホストマシンは、ルーターに「**アドレスマスク要求**」を送信し、「**アドレスマスク応答**」を受信します。

ファイアウォールのルール

グローバル ルール

グローバル ルールは、既にアプリケーションルールが指定されている場合も含め、すべてのネットワーク接続およびアプリケーションに適用できます。

アプリケーション ルール

各アプリケーションに対して、1つまたは複数のルールを指定することができます。ソフォス作成のプリセットルールを使用するか、カスタムルールを作成して、各アプリケーションに対して許可するアクセスを詳細に設定することができます。

グローバル ルールやアプリケーション ルールのデフォルトの設定については、ソフォスのサポートデータベースの文章 57757 を参照してください。

ルールの適用順序

RAW ソケットを使用する接続の場合、グローバル ルールのみがチェックされます。

RAW ソケットを使用しない接続では、「**LAN**」タブで指定したネットワークアドレスへの接続がどうかによってチェックされるルールが異なります。

ネットワークアドレスが「**LAN**」タブに表示されている場合、次のルールがチェックされます。

- アドレスが「**信頼**」と指定されている場合、これ以外のチェックなしで接続が許可されます。
- アドレスが **NetBIOS** と指定されている場合、次の条件を満たす接続すべてにおいて、ファイルとプリンタの共有が許可されます。

接続	ポート	範囲
TCP	リモート	137～139 または 445
TCP	ローカル	137～139 または 445
UDP	リモート	137 または 138
UDP	ローカル	137 または 138

ネットワークアドレスが「**LAN**」タブに表示されていない場合は、他のファイウォールのルールが次の順にチェックされます。

1. 「**LAN**」タブのチェックで接続が許可されなかった **NetBIOS** トラフィックは、「**他のネットワークに対するファイルとプリンタの共有をブロックする**」チェックボックスが選択されている/いないかによって、次のように処理されます。
   - チェックボックスが選択されている場合、トラフィックはブロックされます。
   - チェックボックスが選択されていない場合、トラフィックは残りのルールに従ってブロックされます。
2. 最優先のグローバル ルールは、リストに表示されている順にチェックされます。
3. 接続にまだルールが適用されていない場合、アプリケーション ルールがチェックされます。
4. それでもなお接続が処理されていない場合、通常のグローバル ルールが表示されている順にチェックされます。
5. 接続を処理できるルールが存在しない場合、処理方法は次のとおりです。
   - 「**規定で許可**」モードの場合: 送信方向のトラフィックを許可。
   - 「**規定でブロック**」モードの場合: トラフィックをブロック。
   - 「**対話型**」モードの場合: ユーザーに処理方法を確認。Windows 8 以降の環境でこのモードを使用することはできません。

注
ファイアウォールの動作モードは、デフォルトで「**規定でブロック**」です。

ローカルネットワークの検出

注
Windows 8 以降の環境でこの機能を使用することはできません。

コンピュータのローカルネットワークは、ファイアウォールのルールで指定できます。

ファイアウォールは起動すると、コンピュータのローカルネットワークを判断し、実行中、変更がないか監視します。変更を検出すると、ファイアウォールはローカルネットワークのルールを更新して、新しいローカル ネットワーク アドレスの範囲を指定します。

注意
セカンダリロケーションの設定でローカル ネットワーク ルールを使用する場合は、十分な注意が必要です。社外で使用するモバイル PC の場合、不明なローカルネットワークに接続することがあります。この場合、セカンダリロケーションに対するファイアウォール ルールで、アドレスとしてローカルネットワークを使用するものがあると、不明なトラフィックが許可されてしまう恐れがあります。

グローバル ルール

グローバル ルールを作成する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

重要
グローバル ルールの作成は、ネットワークプロトコルに関する知識がある場合のみ行うことを推奨します。

グローバル ルールは、既にルールが指定されていないすべてのネットワーク接続およびアプリケーションに適用できます。

グローバル ルールを作成する方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**グローバル ルール**」タブをクリックします。
5. 「**追加**」をクリックします。
6. 「**ルール名**」にルールの名前を入力します。
   リスト内のルール名は一意でなければなりません。つまり、同じ名前のグローバル ルールを 2つ作成することはできません。
7. 他のアプリケーション ルールや普通の優先順位のグローバル ルールより優先して適用するには、「**最優先ルール**」チェックボックスをクリックします。
   ルールの適用順序の詳細は、ルールの適用順序 (p. 132)を参照してください。
8. 「**ルールを適用するイベントを選択します**」で、発生時にルールを適用するイベントを選択します。
9. 「**ルールが実行するアクションを選択します**」ボックスで、「**許可する**」または「**ブロックする**」を選択します。
10. 次のいずれかの手順を実行してください。

- 接続の確立中に、同じリモートアドレスから、または同じリモートアドレスへの接続を許可するには、「**コンカレント接続**」を選択します。

  注
  このオプションは、TCP のルールに対してのみ利用できます。同ルールは、デフォルトでステートフル インスペクションが有効になっています。

- 初回の接続に基づいた判断により、リモートコンピュータからの応答を許可するには、「**ステートフル・インスペクション**」を選択します。

  注
  このオプションは、UDP ルールと IP ルールに対してのみ使用できます。

注
Windows 8 以降の環境では常に、**ステートフル インスペクション**が使用され、また「**コンカレント接続**」に対応していないため、このオプションは適用されません。

11. 「**ルールの説明**」で、下線の付いた文字列をクリックします。たとえば、「**TCP (ステートフル)**」リンクをクリックすると、「**プロトコルの選択**」ダイアログボックスが開きます。

グローバル ルールを編集する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

重要
グローバル ルールの変更は、ネットワークプロトコルに関する知識がある場合のみ行うことを推奨します。

グローバル ルールを編集する方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**グローバル ルール**」タブをクリックします。
5. 「**ルール**」リストで、編集するルールをクリックします。
6. 「**編集**」をクリックします。
   グローバル ルールの設定に関する詳細は、ソフォスのサポートデータベースの文章 57757 を参照してください。

グローバル ルールをコピーする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

グローバル ルールをコピーして、ルールのリストに追加する方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**グローバル ルール**」タブをクリックします。
5. 「**ルール**」リストで、コピーするルールをクリックします。
6. 「**コピー**」をクリックします。

グローバル ルールを削除する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**グローバル ルール**」タブをクリックします。
5. 「**ルール**」リストで、削除するルールをクリックします。
6. 「**削除**」をクリックします。

グローバル ルールを適用する順序を変更する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

グローバル ルールは、ルールのリストでの表示に従って、上から順番に適用されます。

グローバル ルールを適用する順序を変更する方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**グローバル ルール**」タブをクリックします。
5. 「**ルール**」リストで、リスト内で上へ移動、または下へ移動するルールをクリックします。
6. 「**上へ移動**」または「**下へ移動**」をクリックします。

アプリケーション ルール

アプリケーション ルールを作成する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

カスタムルールを作成して、各アプリケーションに対して許可するアクセスを詳細に設定する方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**アプリケーション**」タブをクリックします。
5. リストに表示されるアプリケーションを選択し、「**カスタム**」をクリックします。
6. 「**アプリケーションのルール**」ダイアログボックスで、「**追加**」をクリックします。
7. 「**ルール名**」にルールの名前を入力します。
   リスト内のルール名は一意でなければなりません。同じ名前のアプリケーション ルールを 2つ作成することはできませんが、同じ名前のルールを 2つの異なるアプリケーションに指定することはできます。

8. 「**ルールを適用するイベントを選択します**」で、発生時にルールを適用するイベントを選択します。
9. 「**ルールが実行するアクションを選択します**」ボックスで、「**許可する**」または「**ブロックする**」を選択します。
10. 次のいずれかの手順を実行してください。
    - 接続の確立中に、同じリモートアドレスから、または同じリモートアドレスへの接続を許可するには、「**コンカレント接続**」を選択します。

      注
      このオプションは、TCP のルールに対してのみ利用できます。同ルールは、デフォルトでステートフル インスペクションが有効になっています。

    - 初回の接続に基づいた判断により、リモートコンピュータからの応答を許可するには、「**ステートフル・インスペクション**」を選択します。

      注
      このオプションは、UDP ルールと IP ルールに対してのみ使用できます。

    注
    Windows 8 以降の環境では常に、**ステートフル インスペクション**が使用され、また「**コンカレント接続**」に対応していないため、このオプションは適用されません。

11. 「**ルールの説明**」で、下線の付いた文字列をクリックします。たとえば、「**TCP (ステートフル)**」リンクをクリックすると、「**プロトコルの選択**」ダイアログボックスが開きます。

ファイアウォールポリシーからアプリケーション ルールを作成する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「ファイアウォールの詳細ポリシー」の設定ページにて、ファイアウォールポリシーから、直接アプリケーション ルールを作成することができます。

ファイアウォールポリシーからアプリケーション ルールを作成する方法は次のとおりです。

1. 変更するポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「ようこそ」ページで、「**ファイアウォールの詳細ポリシー**」ボタンをクリックします。
3. 表示される「**ファイアウォール ポリシー**」ダイアログボックスで、ファイアウォールを設定するロケーション用の「**環境設定**」ボタンをクリックします。
4. 次のいずれかの手順を実行してください。
    - ファイアウォールポリシーにアプリケーションを追加する場合は、表示されるダイアログボックスの「**アプリケーション**」タブで、「**追加**」をクリックします。

- アプリケーションが隠しプロセスを起動することを許可する場合は、「**プロセス**」タブの上部パネルで「**追加**」をクリックします。
- アプリケーションが RAW ソケットを使用してネットワークにアクセスすることを許可する場合は、「**プロセス**」タブの下部パネルで「**追加**」をクリックします。

「**ファイアウォール ポリシー - アプリケーションの追加**」ダイアログボックスが表示されます。

5. アプリケーションを追加する場合は、「**イベントタイプ**」ボックスで、追加するアプリケーションのタイプ (変更されたアプリケーション、新規アプリケーション、またはファイアウォールポリシーでルールが未設定のアプリケーション) を選択します。
6. 追加するアプリケーション、隠しプロセスの起動を許可するアプリケーション、または RAW ソケットの使用を許可するアプリケーションを一覧から選択し、「**OK**」をクリックします。
ファイアウォールポリシーにアプリケーションが追加されます。

「**アプリケーション**」タブで、アプリケーションは、信頼できるアプリケーションとして追加されます。随時、アプリケーションをブロックしたり、カスタム ルールを作成できます。

アプリケーション ルールを編集する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**アプリケーション**」タブをクリックします。
5. リストに表示されるアプリケーションを選択し、「**カスタム**」をクリックします。
6. 「**アプリケーションのルール**」ダイアログボックスで、「**編集**」をクリックします。
7. 「**ルール名**」にルールの名前を入力します。
リスト内のルール名は一意でなければなりません。同じ名前のアプリケーション ルールを 2つ作成することはできませんが、同じ名前のルールを 2つの異なるアプリケーションに指定することはできます。
8. 「**ルールを適用するイベントを選択します**」で、発生時にルールを適用するイベントを選択します。
9. 「**ルールが実行するアクションを選択します**」ボックスで、「**許可する**」または「**ブロックする**」を選択します。
10. 次のいずれかの手順を実行してください。
    - 接続の確立中に、同じリモートアドレスから、または同じリモートアドレスへの接続を許可するには、「**コンカレント接続**」を選択します。

      注
      このオプションは、TCP のルールに対してのみ利用できます。同ルールは、デフォルトでステートフル インスペクションが有効になっています。

- 初回の接続に基づいた判断により、リモートコンピュータからの応答を許可するには、「**ステートフル・インスペクション**」を選択します。

  注
  このオプションは、UDP ルールと IP ルールに対してのみ使用できます。

注
Windows 8 以降の環境では常に、**ステートフル インスペクション**が使用され、また「**コンカレント接続**」に対応していないため、このオプションは適用されません。

11. 「**ルールの説明**」で、下線の付いた文字列をクリックします。たとえば、「**TCP (ステートフル)**」リンクをクリックすると、「**プロトコルの選択**」ダイアログボックスが開きます。

アプリケーションにプリセットルールを適用する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

プリセットはあらかじめ設定されているアプリケーション ルールの集まりです。各アプリケーション用ルールのリストにプリセットルールを追加する方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**アプリケーション**」タブをクリックします。
5. リストに表示されるアプリケーションを選択し、「**カスタム**」をクリックします。
6. 「**プリセットからのルールの追加**」にカーソルを合わせて、いずれかのプリセットルールをクリックします。

アプリケーション ルールをコピーする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

アプリケーション ルールをコピーして、ルールのリストに追加する方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。

2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**アプリケーション**」タブをクリックします。
5. リストに表示されるアプリケーションを選択し、「**カスタム**」をクリックします。
6. 「**アプリケーションのルール**」ダイアログボックスで、コピーするルールを選択し、「**コピー**」をクリックします。

アプリケーション ルールを削除する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**アプリケーション**」タブをクリックします。
5. リストに表示されるアプリケーションを選択し、「**カスタム**」をクリックします。
6. 「**アプリケーションのルール**」ダイアログボックスで、削除するルールを選択し、「**削除**」をクリックします。

アプリケーション ルールを適用する順序を変更する

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

アプリケーション ルールは、ルールのリストでの表示に従って、上から順番に適用されます。

アプリケーション ルールを適用する順序を変更する方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**アプリケーション**」タブをクリックします。
5. リストに表示されるアプリケーションを選択し、「**カスタム**」をクリックします。

6. 「**アプリケーションのルール**」ダイアログボックスの「**ルール**」リストで、リスト内で上へ移動、または下へ移動するルールをクリックします。
7. 「**上へ移動**」または「**下へ移動**」をクリックします。

接続先の検出機能

接続先の検出機能は、接続先に応じてコンピュータの各ネットワークアダプタに異なるファイアウォールの設定を適用する Sophos Client Firewall の機能です。

この機能は主に自宅勤務者が使用するモバイル PC に対して使います。自宅勤務者は以下のような2種類のネットワーク接続を同時利用します。

- 業務利用: VPN クライアントおよび**仮想ネットワークアダプタ**を通じて社内ネットワークに接続します。
- 業務外の利用: ネットワークケーブルおよび**物理ネットワークアダプタ**を通じて個々の ISP に接続します。

このような場合、仮想オフィスの接続には業務用の設定を適用し、業務外の ISP 接続には業務外用の設定 (通常、厳しい制限をかけます) を適用する必要があります。

注
業務外用の設定には、「仮想オフィス」の接続を許可するための詳細なルールが必要です。

接続先の検出機能の設定について

1. プライマリロケーションのゲートウェイ MAC アドレスまたはドメイン名のリストを作成します。通常、どちらも社内ネットワークのものです。
2. プライマリロケーションで使用するファイアウォールの設定を作成します。通常、セカンダリロケーションに比べ少ない制限を設定します。
3. セカンダリロケーション用のファイアウォールの設定を作成します。通常、プライマリロケーションに比べ厳しい制限を設定します。
4. 適用する設定を選択します。

お使いの検出方法に応じて、コンピュータのネットワークアダプタの DNS アドレスまたはゲートウェイアドレスをファイアウォールが取得し、作成したアドレスのリストと照合します。

- ネットワークアダプタと一致するアドレスがリストにある場合、そのアダプタには**プライマリロケーション**用の設定が適用されます。
- ネットワークアダプタと一致するアドレスがリストにない場合は、そのアダプタには**セカンダリロケーション**用のポリシーが適用されます。

重要
セカンダリロケーション用の設定では、次のいずれの条件にも該当する場合、「**対話型**」モードから「**規定でブロック**」モードに切り替えられます。

- 両方の接続先がアクティブな状態である。
- プライマリロケーション用の設定が対話型モードになっていない。

プライマリロケーションを定義する

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。

3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**接続先の検出**」タブをクリックします。
5. 「**検出方法**」パネルで、プライマリロケーションを定義するオプションを選択し、横にある「**環境設定**」をクリックします。

オプション	説明
DNS 参照を使用する	各プライマリロケーションのドメイン名と、対応する IP アドレスをリストに追加します。
ゲートウェイの MAC アドレスを使用する	各プライマリロケーションのゲートウェイの MAC アドレスをリストに追加します。

6. 画面の指示に従います。

セカンダリロケーション用の設定を作成する

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**セカンダリロケーションを設定する**」チェックボックスを選択します。

セカンダリロケーション用の設定を行ってください。操作方法の詳細は、詳細設定ページを開く (p. 121) を参照してください。

注意
セカンダリロケーションの設定でローカル ネットワーク ルールを使用する場合は、十分な注意が必要です。社外で使用するモバイル PC の場合、不明なローカルネットワークに接続することがあります。この場合、セカンダリロケーションに対するファイアウォール ルールで、アドレスとしてローカルネットワークを使用するものがあると、不明なトラフィックが許可されてしまう恐れがあります。

適用する設定を選択する

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**全般**」タブの「**コンピュータの接続先と設定内容**」セクションで次のいずれかのオプションをクリックします。

オプション	**説明**
検出された接続場所に応じた設定内容	ファイアウォールは、接続先の検出機能の設定内容に応じて、各ネットワーク接続に対してプライマリロケーションまたはセカンダリロケーション用の設定を適用します (接続先の検出機能の設定について (p. 141)を参照)。

オプション	説明
プライマリロケーション用の設定内容	ファイアウォールは、すべてのネットワーク接続に対してプライマリロケーション用の設定を適用します。
セカンダリロケーション用の設定内容	ファイアウォールは、すべてのネットワーク接続に対してセカンダリロケーション用の設定を適用します。

ファイアウォールのレポート機能

デフォルトで、エンドポイントコンピュータ上のファイアウォールは、Enterprise Console に、ステータスの変化、イベント、およびエラーをレポートします。

ファイアウォールのステータスの変更

ファイアウォールのステータスの変更の種類は次のとおりです。

- 動作モードの変更
- ソフトウェアバージョンの変更
- すべてのトラフィックを許可する設定の変更
- ファイアウォールのポリシーコンプライアンスの変更

対話型モードでファイアウォールを使用している場合、**Enterprise Console** から適用されるポリシーと異なった設定内容がローカルマシンに適用されることがあります。この場合、特定のファイアウォール設定に変更を加えた際、Enterprise Console に「ポリシーと異なる」という警告が**送信されないよう**設定することができます。

詳細は、ローカルマシンで行った変更のレポートを有効/無効にする (p. 143)を参照してください。

ファイアウォールのイベント

エンドポイントコンピュータ上の OS や不明なアプリケーションが、ネットワークを介して他のコンピュータと通信しようとすることをイベントと言います。

ファイアウォールが、イベントを Enterprise Console にレポートしないよう設定できます。

詳細は、不明なネットワークのレポートを無効にする (p. 144)を参照してください。

ローカルマシンで行った変更のレポートを有効/無効にする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

エンドポイントコンピュータのファイアウォールの環境設定がポリシーと異なる場合は、**ローカルマシンで行った変更のレポートを無効にする**ことができます。

注
Windows 8 以降の環境でこのオプションを使用することはできません。

ローカルマシンで行った変更のレポートを無効にすると、グローバル ルール、アプリケーション、プロセス、またはチェックサムがローカルマシンで変更された際、Enterprise Console に「ポリシーと異なる」という警告が送信されなくなります。ここで設定する内容は、対話型ダイアログボックスを使って変更可能なので、対話型モードで操作を行う場合など、この設定を行うと便利です。

エンドポイントコンピュータのファイアウォールの環境設定をポリシーに準拠させる必要がある場合は、**ローカルマシンで行った変更のレポートを有効にしてください。**

ローカルマシンで行った変更のレポートを無効にする方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**全般**」タブをクリックします。
5. 「**レポート**」パネルで次のいずれかを実行します。
   - ローカルマシンで行われた変更のレポートを有効にするには、「**グローバル ルール、アプリケーション、プロセス、またはチェックサムがローカルマシンで変更された場合、管理コンソールに警告を表示する**」チェックボックスを選択します。
   - ローカルマシンで行われた変更のレポートを無効にするには、「**グローバル ルール、アプリケーション、プロセス、またはチェックサムがローカルマシンで変更された場合、管理コンソールに警告を表示する**」チェックボックスの選択を外します。

不明なネットワークのレポートを無効にする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

エンドポイントコンピュータのファイアウォールが、不明なネットワークを Enterprise Console にレポートしないよう設定できます。ファイアウォールは、どのルールにも該当しないトラフィックを不明と見なします。

エンドポイントコンピュータのファイアウォールが、不明なネットワークを Enterprise Console にレポートしないよう設定する方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールのロケーションに対応する「**環境設定**」をクリックします。
4. 「**全般**」タブをクリックします。

5. 「**ブロック**」パネルで、「**チェックサムを使用してアプリケーションを認証する**」チェックボックスを選択します。
6. 「**レポート**」パネルで、「**管理コンソールに不明なアプリケーションとトラフィックをレポートする**」チェックボックスを選択から外します。

ファイアウォールエラーのレポートを無効にする

重要
ファイアウォールエラーのレポートは、常時無効に設定しておかないことを推奨します。レポートは、必要な場合のみ無効にするようにしてください。

エンドポイントコンピュータ上のファイアウォールが、エラーを Enterprise Console にレポートしないようにする方法は次のとおりです。

1. 変更するファイアウォールポリシーをダブルクリックします。
2. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。
3. 「**環境設定**」パネルで、設定するファイアウォールの口ケーションに対応する「**環境設定**」をクリックします。
4. 「**全般**」タブをクリックします。
5. 「**レポート**」パネルで、「**管理コンソールにエラーをレポートする**」チェックボックスを選択から外します。

ファイアウォールの設定をインポート、エクスポートする

注
ロールベースの管理を利用している場合は次の点に注意してください。

- ファイアウォールポリシーを設定するには、「**ポリシー設定 - ファイアウォール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ファイアウォールの全般的な設定やルールを、環境設定ファイル (*.conf) としてインポート、エクスポートすることができます。この機能を使って実行できる操作は次のとおりです。

- ファイアウォールの環境設定のバックアップを作成し、復旧できるようにする。
- 1台のコンピュータで作成したアプリケーション ルールをインポートし、それを使用して、同じアプリケーションの組み合わせを実行している他のコンピュータに対するポリシーを作成する。
- 数台のコンピュータで作成して設定内容を結合し、ネットワーク上の 1つまたは複数のコンピュータのグループに対して有効なポリシーを作成する。

ファイアウォールの設定をインポート、エクスポートする方法は次のとおりです。

1. 設定するコンピュータのグループに、どのファイアウォールポリシーが指定されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**ファイアウォール**」をダブルクリックし、インポートまたはエクスポートするポリシーをダブルクリックします。
3. 「**ファイアウォール ポリシー**」ウィザードの「**ようこそ**」ページで、「**ファイアウォールの詳細ポリシー**」をクリックします。

4. 「**ファイアウォール ポリシー**」ダイアログボックスで、「**全般**」タブの「**環境設定の管理**」パネルで、「**インポート**」または「**エクスポート**」をクリックします。

7.3 アプリケーション コントロール ポリシー

Enterprise Console では、アプリケーション コントロール機能で「管理対象アプリケーション」、すなわち、セキュリティ脅威はもたらさないものの、管理者が業務上の使用は不適切と判断する正規のアプリケーションを検知・ブロックすることができます。このようなアプリケーションには、インスタント メッセージング (IM) クライアント、VoIP クライアント、デジタル画像ソフト、メディアプレーヤー、ブラウザプラグインなどがあります。

注
このオプションは、 Sophos Endpoint Security and Control for Windows のみに適用されます。

各グループごとにフレキシブルに、アプリケーションをブロックしたり、認証できます。たとえば、社内で使用しているデスクトップに対して VoIP の実行をブロックしつつ、社外で使用しているモバイル PC に対しては、その使用を認証することができます。

管理対象アプリケーションのリストは、ソフォスが定期的に更新し、提供しています。お客様自身でリストに新しいアプリケーションを追加することはできません。新たな正規アプリケーションをアプリケーションコントロールの対象にする必要がある場合は、ソフォスまでご連絡ください。

詳細は、サポートデータベースの文章 63656 を参照してください。

ここでは、社内ネットワークでの使用をコントロールするアプリケーションを選択する方法や、そのようなアプリケーションの検索を設定する方法について説明します。

注
ロールベースの管理を利用している場合は次の点に注意してください。

- アプリケーション コントロール ポリシーを設定するには、「**ポリシー設定 - アプリケーション コントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

アプリケーション コントロールのイベント

ネットワークでの管理対象アプリケーションの検出など、アプリケーション コントロールに関するイベントが発生すると、アプリケーション コントロールのイベントログに書き込まれます。ログは、Enterprise Console で表示できます。詳細は、アプリケーション コントロールのイベントを表示する (p. 199)を参照してください。

過去 1週間で、しきい値を超える数のイベントが発生したコンピュータの台数は、ダッシュボードに表示されます。

また、アプリケーション コントロールのイベントが発生した場合に、特定の受信者に警告を送信するよう設定できます。詳細は、アプリケーション コントロールの警告やメッセージを設定する (p. 193)を参照してください。

7.3.1 管理対象アプリケーションを選択する

ロールベースの管理を利用している場合は次の点に注意してください。

- アプリケーション コントロール ポリシーを設定するには、「**ポリシー設定 - アプリケーション コントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、すべてのアプリケーションが許可されています。アプリケーション コントロール機能で、使用をコントロールするアプリケーションを選択する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのアプリケーション コントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**アプリケーション コントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**アプリケーション コントロール ポリシー**」ダイアログボックスで、「**認証**」タブをクリックします。
4. 「**アプリケーションの種類**」(たとえば「**ファイル交換**」など) を選択します。
   選択したタイプに属するアプリケーションの一覧が「**認証済み**」リストに表示されます。
   - 特定のアプリケーションをブロックするには、それを選択して、以下のような「追加」ボタンをクリックし、「**ブロック**」リストへ移動します。

   - 今後ソフォスによって追加される特定のタイプの新規アプリケーションすべての使用をブロックする場合は、「**今後ソフォスが追加するアプリケーションすべて**」を「**ブロック**」リストに移動します。
   - 特定の種類のアプリケーションすべてをブロックするには、以下のような「すべて追加」ボタンをクリックして、すべてのアプリケーションを 「**認証済み**」リストから「**ブロック**」リストへ移動します。

5. 「**アプリケーション コントロール ポリシー**」ダイアログボックスの「**検索**」タブで、管理対象アプリケーションの検索が有効になっていることを確認してください。(詳細は、管理対象アプリケーションを検索する (p. 147) を参照してください。)「**OK**」をクリックします。

7.3.2 管理対象アプリケーションを検索する

ロールベースの管理を利用している場合は次の点に注意してください。

- アプリケーション コントロール ポリシーを設定するには、「**ポリシー設定 - アプリケーション コントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Sophos Endpoint Security and Control を設定して、ネットワーク上で使用をコントロールするアプリケーションをオンアクセス検索できます。

1. 設定するコンピュータのグループ (複数可) に、どのアプリケーション コントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**アプリケーション コントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
   「**アプリケーション コントロール ポリシー**」ダイアログボックスが表示されます。
3. 「**検索**」タブで、オプションを次のように設定します。
   - オンアクセス検索を有効にするには、「**オンアクセス検索を有効にする**」チェックボックスを選択します。アプリケーションの検出はするものの、オンアクセスでのブロックは実行しない場合は、「**検出するが、実行は許可する**」チェックボックスを選択します。
   - オンデマンド/スケジュール検索を有効にするには、「**オンデマンド/スケジュール検索を有効にする**」チェックボックスを選択します。

   注
   ウイルス対策および HIPS ポリシーの設定内容で、検索するファイルが指定されます (拡張子と除外の設定など)。

ネットワークに接続されているコンピュータで検出された管理対象アプリケーションを削除する場合は、不要な管理対象アプリケーションをアンインストールする (p. 148)の説明に従ってください。

また、グループ内のコンピュータでアプリケーション コントロール機能で管理対象アプリケーションが検出された場合、特定のユーザーにメールで警告を送信することができます。手順については、アプリケーション コントロールの警告やメッセージを設定する (p. 193)を参照してください。

7.3.3 不要な管理対象アプリケーションをアンインストールする

管理対象アプリケーションのアンインストールを開始する前に、必ず、管理対象アプリケーションのオンアクセス検索を無効にしてください。オンアクセス検索では、アプリケーションのインストールやアンインストールに使用するプログラムがブロックされるので、無効にしない場合、アンインストールが実行できなくなる恐れがあります。

アプリケーションは、次のいずれか 1つの方法でアンインストールできます。

- 各コンピュータで、対象の製品用のアンインストーラを実行する。通常、Windows の「コントロール パネル」の「プログラムの追加と削除」から実行できます。
- サーバーから、通常使用しているスクリプトや管理ツールを使用して、ネットワーク上のコンピュータにて、対象の製品用のアンインストーラを実行する。

次に、管理対象アプリケーションのオンアクセス検索を有効にします。

7.4 データコントロール ポリシー

注
この機能はすべてのライセンスには含まれていません。利用するには追加購入が必要となります。詳細は、http://www.sophos.com/ja-jp/products/complete/comparison.aspxを参照してください。

データコントロールは、機密情報を含むファイルの転送を監視・制限し、クライアントマシンからのデータ流出事故を防止する機能です。機能を有効にするには、データコントロールのルールを作成し、**データコントロール** ポリシーに追加します。

特定のデバイス (リムーバブル ストレージ デバイスなど) へのデータ転送や、特定のアプリケーション (メールクライアント、Web ブラウザなど) によるデータ転送を監視・コントロールできます。

データコントロールポリシーは、SophosLabs (ソフォスラボ) が作成・管理する機密データの定義ライブラリ (コンテンツ コントロール リスト) を利用することで、迅速に定義・ロールアウトできます。ライブラリには、主に個人を特定できる情報の定義データが収録されていますが、他の一般的なデータ構造も含まれています。Enterprise Console におけるコンテンツ コントロール リストの使用方法については、次の説明を参照してください。

7.4.1 データコントロールの機能

データコントロールは、主に人為的ミスなどで生じる機密情報の流出事故を検知する機能です。たとえば、Web ベースのメール機能で、機密情報が含まれるファイルを自宅に送信する行為などが対象になります。

データコントロール機能で、コンピュータから、ストレージデバイスやインターネットに接続するアプリケーションへのファイルの転送を監視・制御することができます。

- **ストレージデバイス:** データコントロール機能は、Windows エクスプローラを使って監視対象ストレージデバイスにコピーされるすべてのファイルをブロックします (Windows のデスクトップでファイルをコピーした場合も同様です)。ただし、Microsoft Word など、アプリケーションから直接ファイルを保存した場合や、コマンドプロンプトでファイルを転送した場合は、ブロックされません。

  管理対象ストレージデバイスへのファイル転送を、すべて Windows エクスプローラを使って実行させるようにするには、「**ユーザーの同意で転送を許可し、イベントをログに記録する**」アクション、または「**転送をブロックし、イベントをログに記録する**」アクションを利用します。どちらの場合でも、アプリケーションから直接ファイルを保存しようとしたり、コマンドプロンプトでファイルを転送しようとすると、データコントロール機能でブロックされます。そして、Windows エクスプローラを使ってファイル転送を行うよう、デスクトップ警告が表示されます。

  データコントロール ポリシーで、「**ファイル転送を許可し、イベントをログに記録する**」アクションに関するルールのみが設定されている場合は、アプリケーションで直接ファイルを保存しようとしたり、コマンドプロンプトからファイルを転送しようとしても、ファイルはブロックされません。この設定では、ユーザーが制限なしでストレージデバイスを使うことができます。しかし、Windows エクスプローラを使ってファイル転送を行ったときは、データコントロールのイベントが記録されます。

注
アプリケーションの監視はこの制限の対象ではありません。

- **アプリケーション:** ユーザーが実行するファイルのアップロードだけを監視するため、一部のシステムファイルの保存先は、データコントロールによる監視の対象から除外されています。これによって、ユーザーがファイルをアップロードしたときではなく、アプリケーションが環境設定ファイルを開いたときに、データコントロールのイベントが生成される可能性が大幅に削減されます。

重要
アプリケーションによって環境設定ファイルが開かれるために誤ったイベントが生成される場合は、通常、除外するパスを追加したり、データコントロールのルールを緩和することで問題は解決します。詳細はソフォスのサポートデータベースの文章 113024 を参照してください。

注
オンアクセス検索の除外は、常にデータコントロールに適用されません。

オンアクセス検索の除外設定がデータコントロールに適用される条件とは？

ウイルス対策および HIPS ポリシーで設定したオンサクセス検索の除外は、どのようにファイルがコピー/移動されたか、あるいはどの場所へコピー/移動されたかに応じて、データコントロールに適用されます。

たとえば、メールクライアント、Web ブラウザ、IM (インスタントメッセージング) など、監視対象のアプリケーションを使用してファイルがアップロードされたときや、添付されたときに、オンアクセス検索の除外設定がデータコントロールに**適用されます**。オンアクセス検索の対象から項目を除外する方法の詳細は、オンアクセス検索の対象から項目を除外する (p. 87)を参照してください。

重要
オンアクセス検索の対象からリモートファイルを除外した場合、ネットワーク上のファイルを監視対象アプリケーション (メールクライアントや Web ブラウザなど) にアップロードしたり、添付したりした際、それらのファイルに対してデータコントロールで検索が実行されません。詳細は、アップロードされたファイルや添付ファイルが、データコントロールで検索されない (p. 230)も参照してください。

Windows エクスプローラを使用してファイルをコピー/移動した場合、オンアクセス検索の除外設定はデータコントロールに**適用されません**。結果として、たとえば、USB などのストレージデバイスにファイルをコピーした場合や、ネットワーク上にファイルをコピー/移動した場合、これらのファイルに対して検索が実行されます。オンアクセス検索の対象からリモートファイルを除外していたとしても、すべてのファイルに対して検索が実行されます。

注
圧縮ファイルをネットワークにコピー/移動する際、処理に時間がかかることがあります。ネットワークの接続状況にもよりますが、100MB のデータを処理するのに 1分以上かかることもあります。これは、圧縮ファイルの検索は、通常のファイルの検索に比べ、時間がかかるためです。

データコントロール ポリシー

データコントロール機能でファイルの転送を監視・制御するには、データコントロール ポリシーで対象となるファイルを定義し、ネットワーク上の各コンピュータのグループに適用します。

重要
データコントロール機能は、Windows 2008 の Server Core には対応していないため、この OS を実行しているコンピュータでは無効に設定する必要があります。Windows 2008 の Server Core を実行するコンピュータをデータコントロールの対象から除外するには、データコントロールを無効に設定したデータコントロール ポリシーが適用されているグループに配置してください。詳細は、データコントロールを有効/無効にする (p. 154)を参照してください。

データコントロール ポリシーには、1つ以上のルールが含まれており、データコントロールの対象や、ルールが一致したときに実行するアクションなどを設定します。1つのデータコントロールのルールは、複数のポリシーに追加できます。

複数のルールを含むデータコントロール ポリシーの場合、ポリシー内のルールのどれか 1つにでも一致したファイルは、ポリシーに準拠していないと判定されます。

データコントロールのルールの条件

データコントロールのルールの条件には、転送先、ファイル名、ファイル拡張子、ファイルタイプ、またはファイルコンテンツなどがあります。

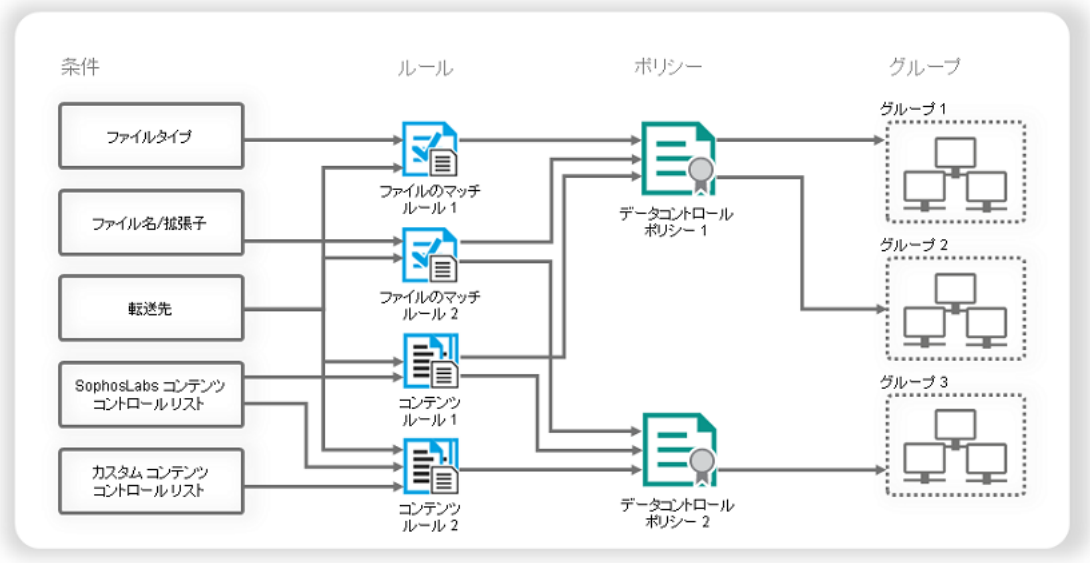
転送先には、デバイス (例: USB フラッシュメモリなどのリムーバブル ストレージ デバイス) や、アプリケーション (例: インターネットブラウザおよびメールクライアント) があります。

ファイルコンテンツの一致条件は、コンテンツ コントロール リストで定義されています。このリストは、データを XML 形式のデータ構造としてまとめたものです。SophosLabs (ソフォスラボ) は、データコントロールのルールに利用できる豊富な内容の各種コンテンツ コントロール リストを提供しています。

ファイルに適用するデータコントロールのルールと条件について、詳細はデータコントロールのルールについて (p. 152)を参照してください。

ファイルコンテンツを定義するコンテンツ コントロール リスト (CCL) について、詳細はコンテンツ コントロール リストについて (p. 153)を参照してください。

データコントロール



データコントロールのルールのアクション

データコントロールで、ルールで設定されている条件すべてが検出されると、ルールで指定されているアクションが実行され、イベントがログに記録されます。次のいずれかのアクションを指定できます。

- ファイル転送を許可し、イベントをログに記録する
- ユーザーの同意で転送を許可し、イベントをログに記録する
- 転送をブロックし、イベントをログに記録する

あるファイルが 2つのデータコントロールのルールに一致し、それぞれのルールで異なるアクションが設定されている場合は、より制限の厳しいアクションを含むルール適用されます。ユーザーの同意で転送を許可するルールよりも、転送をブロックするルールの方が優先されます。ファイル転送を許可するルールよりも、ユーザーの同意で転送を許可するルールの方が優先されます。

デフォルトで、ルールに一致しファイル転送がブロックされた場合や、ファイル転送にユーザーの同意が必要な場合は、エンドポイントコンピュータのデスクトップにメッセージが表示されます。メッセージには、適用されたルールが表示されます。ファイル転送の際や、転送をブロックした際に表示する確認メッセージには、オリジナルのメッセージを付け加えることもできます。詳細は、データコントロールの警告やメッセージを設定する (p. 194)を参照してください。

7.4.2 データコントロールのルールについて

データコントロールのルールには、検出条件、ルールが一致したときに実行するアクション、および除外するファイルを指定します。

ルールは、独自のものを作成したり、あらかじめ用意されているものを使用できます。複数用意されている定義済みのデータコントロールのルールは、そのまますぐ使うことはもちろん、要件に合わせて設定を変更することもできます。これらのルールはサンプルとして用意されているため、更新されることはありません。

データコントロールのルールは 2種類あります。1つはファイルのマッチルールで、もう 1つはコンテンツルールです。

ファイルのマッチルール

ファイルのマッチルールは、ユーザーが特定のファイル名や種類 (スプレッドシートなど正式なファイルタイプのカテゴリ) のファイルを、特定の場所に転送しようとした場合に実行するアクション (リムーバブル ストレージ デバイスへのデータ転送のブロックなど) を指定します。

データコントロール機能では、150種類以上のファイル形式に対応するファイルタイプが定義されています。今後、時折、新たな対応ファイルタイプが追加される可能性もあります。この場合、新しいファイルタイプは、該当するカテゴリが使用されているすべてのデータコントロールのルールに自動的に追加されます。

正式に定義されていないファイルタイプを認識する場合は、ファイル拡張子を使います。

コンテンツルール

コンテンツルールは、1つ以上のコンテンツコントロールリストを含むルールで、ユーザーがすべてのコンテンツ コントロール リストに一致するデータを、特定の場所に転送しようとした場合に実行するアクションを設定します。

7.4.3 コンテンツ コントロール リストについて

コンテンツ コントロール リスト (CCL) は、ファイルコンテンツのデータ構造のパターンをまとめたリストです。コンテンツ コントロール リストでは、1種類のデータタイプ (住所や社会保障番号など) や、数種類のデータタイプの組み合わせ (「confidential」という用語を含むプロジェクト名など) を指定できます。

あらかじめ定義されている SophosLabs コンテンツ コントロール リストをそのまま使用することはもちろん、独自のコンテンツ コントロール リストを作成することもできます。

SophosLabs コンテンツ コントロール リストでは、クレジットカード番号、社会保障番号、住所、メールアドレスなど、一般的な財務関連情報や個人情報のデータタイプが詳細に定義されています。チェックサムなどの高度な技術で機密情報をより正確に検出できます。

お客様自身で SophosLabs コンテンツ コントロール リストを編集することはできません。SophosLabs コンテンツ コントロール リストに変更を加える必要がある場合は、ソフォスまでご連絡ください。詳細は、ソフォスのサポートデータベースの文章 51976 を参照してください。

注
現バージョンのコンテンツ コントロール リストでは、日本語、中国語などの 2バイト文字には正式に対応していません。しかし、コンテンツ コントロール リストのエディタに、2バイト文字を入力することは可能です。

SophosLabs コンテンツ コントロール リストに対してデータ量を設定する

ほとんどの SophosLabs コンテンツ コントロール リストでは、データ量が指定されています。

データ量はコンテンツ コントロール リストにおける主要なデータタイプの量のことで、設定値がファイルで検出されると、コンテンツ コントロール リストが照会されます。SophosLabs コンテンツ コントロール リストのデータ量は、対象のリストが属するコンテンツルールで編集できます。

データ量を使ってデータコントロールのルールを詳細に設定することで、機密情報を含まないドキュメント (例: 1件の住所または 1件以上の電話番号を含むレターなど) のブロックを防止できます。検索対象のデータ量を 1つの住所にすると、数千件のドキュメントがルールと一致する可能性があり、結果としてデータコントロールのイベントが発生します。顧客リストの流出を防止する場合は、50件を超える住所を含む場合のみ、ドキュメントのデータ転送を検出するなどの対策が必要です。ただし、クレジットカードなど他の項目に関しては、検索対象のデータ量を 1件に設定することを推奨します。

7.4.4 データコントロールのイベントについて

データコントロールのイベント (機密情報を含むファイルの USB メモリへのコピーなど) が発生すると、Enterprise Console に情報が送信されます。送信されたイベントは、「**データコントロール - イベントビューア**」で表示できます。イベントは各エンドポイントのローカルディスクにもログ出力され、適切な権限がある場合は、Sophos Endpoint Security and Control で表示できます。

注
各エンドポイントコンピュータが Enterprise Console に送信できるデータコントロール イベントの件数は、1時間につき最大 50件です。すべてのイベントは、各エンドポイントコンピュータのローカルディスクにログ出力されます。

「**データコントロール - イベントビューア**」ダイアログボックスでは、必要な情報をフィルタで抽出できます。また、データコントロールのイベントの一覧をファイルに出力できます。詳細は、データコントロールのイベントについて (p. 154)、およびイベントの一覧をファイルに出力する (p. 208)を参照してください。

過去 1週間で、データコントロールのイベントが、しきい値を超えて発生したコンピュータの台数は、ダッシュボードに表示されます。しきい値の設定方法については、ダッシュボードのパネル (p. 4)を参照してください。

また、データコントロールのイベントが発生した場合に、特定の受信者に警告を送信するよう設定できます。詳細は、データコントロールの警告やメッセージを設定する (p. 194)を参照してください。

7.4.5 データコントロールを有効/無効にする

ロールベースの管理を利用している場合は次の点に注意してください。

- データコントロール ポリシーを設定するには、「**ポリシー設定 - データコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、データコントロールは無効になっています。ネットワーク経由のファイル転送を監視・制限するルールも指定されていません。

データコントロールを有効にする方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのデータコントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。

2. 「**ポリシー**」ペインで、「**データコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
   「**データコントロール ポリシー**」ダイアログボックスが表示されます。
3. 「**ポリシーのルール**」タブで、「**データコントロールを有効にする**」チェックボックスを選択します。
4. 「**ルールの追加**」ボタンをクリックします。「**データコントロール ルールの管理**」ダイアログボックスで、ポリシーに追加するルールを選択し、「**OK**」をクリックします。

   重要
   データコントロールのルールが全く追加されていない場合は、追加するまでファイル転送の監視や制限は実行されません。

後で、データコントロールを無効にする場合は、「**データコントロールを有効にする**」チェックボックスの選択を外します。

7.4.6 ファイルのマッチルールを作成する

ロールベースの管理を利用している場合は次の点に注意してください。

- データコントロールのルールを作成、または編集するには、「**データコントロール設定**」権限が必要です。
- データコントロール ポリシーを設定するには、「**ポリシー設定 - データコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

ファイルのマッチルールの概要は、データコントロールのルールについて (p. 152)を参照してください。

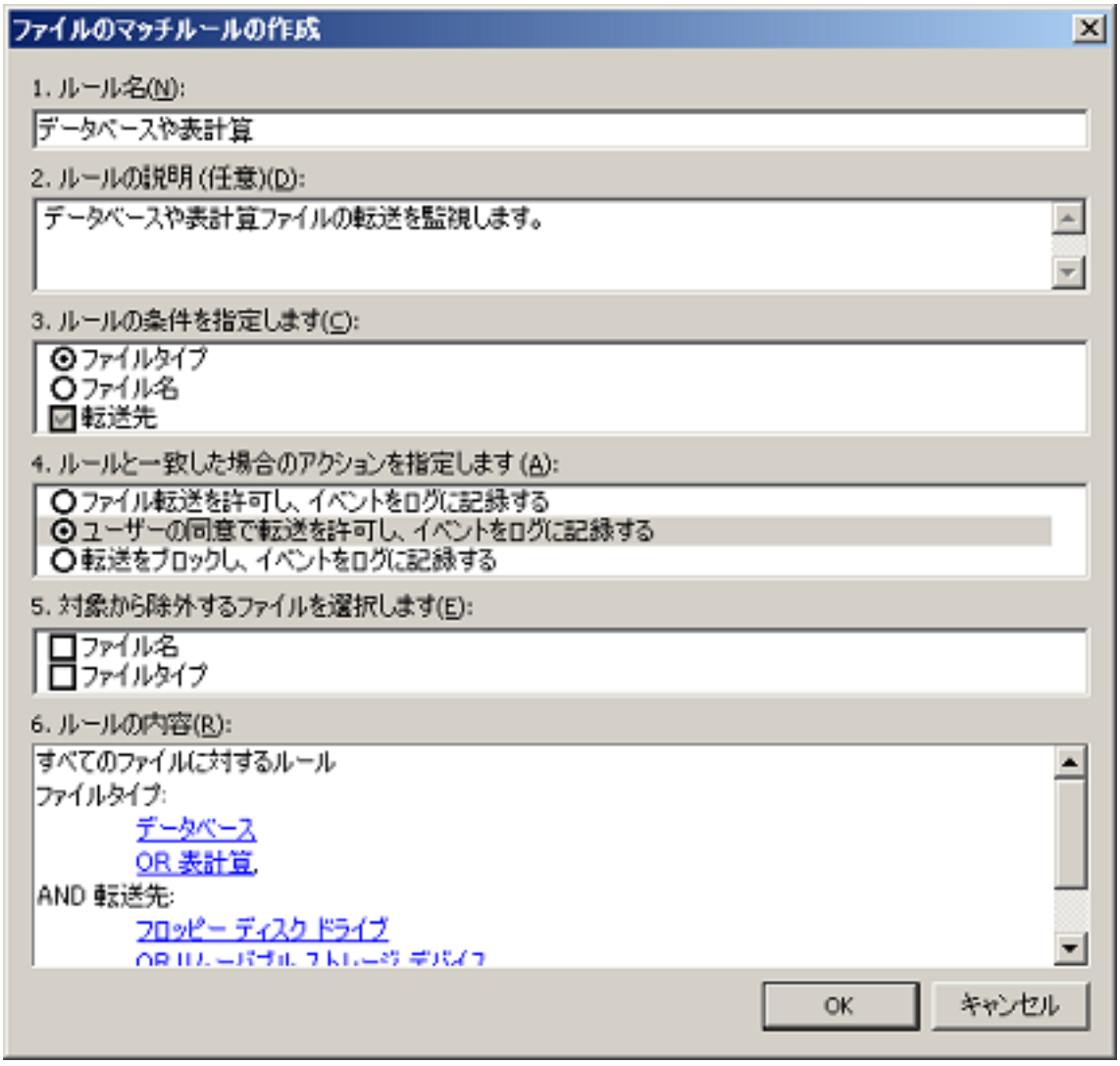
ファイルのマッチルールを作成し、データコントロール ポリシーに追加する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのデータコントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
   または、「**ツール**」メニューからルールを作成し、ポリシー (複数可) に追加することもできます。「**ツール**」メニューで、「**データコントロールの管理**」にカーソルを合わせて「**データコントロールのルール**」をクリックします。そして、ステップ 4～10 を実行します。
2. 「**ポリシー**」ペインで、「**データコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**データコントロール ポリシー**」ダイアログボックスの「**ポリシーのルール**」タブで、「**データコントロールを有効にする**」チェックボックスが選択されていることを確認し、「**ルールの管理**」をクリックします。
4. 「**データコントロール ルールの管理**」ダイアログボックスで、「**ファイルのマッチルールの追加**」ボタンをクリックします。
5. 「**ファイルのマッチルールの作成**」ダイアログボックスの「**ルール名**」欄にルールの名前を入力します。
6. 必要に応じて、「**ルールの説明 (任意)**」欄にルールの説明を入力します。
7. 「**ルールの条件を指定します**」欄で、ルールの条件を選択します。
   転送先の条件項目は自動的に選択されますが、この項目の設定は必須です。

デフォルトで、すべてのファイルタイプが検索されます。特定の種類のファイルだけを検索する場合は、「**ファイルタイプ**」を選択します。そして、ステップ 10 の説明に従って条件を設定します。

8. 「**ルールと一致した場合のアクションを指定します**」欄で、アクションを選択します。
9. データコントロールの対象から一部のファイルを除外する場合は、「**対象から除外するファイルを選択します**」欄で、「**ファイル名**」または「**ファイルタイプ**」チェックボックスを選択します。
10. 「**ルールの内容**」欄で、下線が付いている各項目をクリックし、ルールの条件を設定します。たとえば、「**転送先の選択**」をクリックすると、「**転送先タイプのマッチ条件**」ダイアログボックスが開き、データ転送を制限するデバイスやアプリケーションを選択できます。

    下線付きの各項目に対して条件を選択、または入力します。



    「**OK**」をクリックします。

    新しいルールが「**データコントロール ルールの管理**」ダイアログボックスに表示されます。

11. ルールをポリシーに追加するには、ルール名の横のチェックボックスを選択し、「**OK**」をクリックします。

    データコントロール ポリシーにルールが追加されます。

データコントロール ポリシーに適用されているルールに一致した際に、当該のユーザーに警告とメッセージを送信するよう設定できます。詳細は、データコントロールの警告やメッセージを設定する (p. 194)を参照してください。

7.4.7 コンテンツルールを作成する

ロールベースの管理を利用している場合は次の点に注意してください。

- データコントロールのルールや、コンテンツ コントロール リストを作成、または編集するには、「**データコントロール設定**」権限が必要です。
- データコントロール ポリシーを設定するには、「**ポリシー設定 - データコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

コンテンツルールとコンテンツ コントロール リストの概要は、データコントロールのルールについて (p. 152)を参照してください。

コンテンツルールを作成し、データコントロール ポリシーに追加する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのデータコントロール ポリシーが適用されているか確認してください。

   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。

   または、「**ツール**」メニューからルールを作成し、ポリシー (複数可) に追加することもできます。「**ツール**」メニューで、「**データコントロールの管理**」にカーソルを合わせて「**データコントロールのルール**」をクリックします。そして、ステップ 4～13 を実行します。
2. 「**ポリシー**」ペインで、「**データコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**データコントロール ポリシー**」ダイアログボックスの「**ポリシーのルール**」タブで、「**データコントロールを有効にする**」チェックボックスが選択されていることを確認し、「**ルールの管理**」をクリックします。
4. 「**データコントロール ルールの管理**」ダイアログボックスで、「**コンテンツルールの追加**」ボタンをクリックします。
5. 「**コンテンツルールの作成**」ダイアログボックスの「**ルール名**」欄にルールの名前を入力します。
6. 必要に応じて、「**ルールの説明 (任意)**」欄にルールの説明を入力します。
7. 「**ルールの条件を指定します**」欄では、ファイルコンテンツと転送先の条件項目が自動的に選択されています。どちらも必須設定項目です。
8. 「**ルールと一致した場合のアクションを指定します**」欄で、アクションを選択します。
9. データコントロールの対象から一部のファイルを除外する場合は、「**対象から除外するファイルを選択します**」欄で、「**ファイル名**」または「**ファイルタイプ**」チェックボックスを選択します。
10. 「**ルールの内容**」欄で、下線付きの「含まれるデータ」をクリックします。
11. 「**コンテンツ コントロール リストの管理**」ダイアログボックスで、ルールに含めるコンテンツ コントロール リストを選択します。

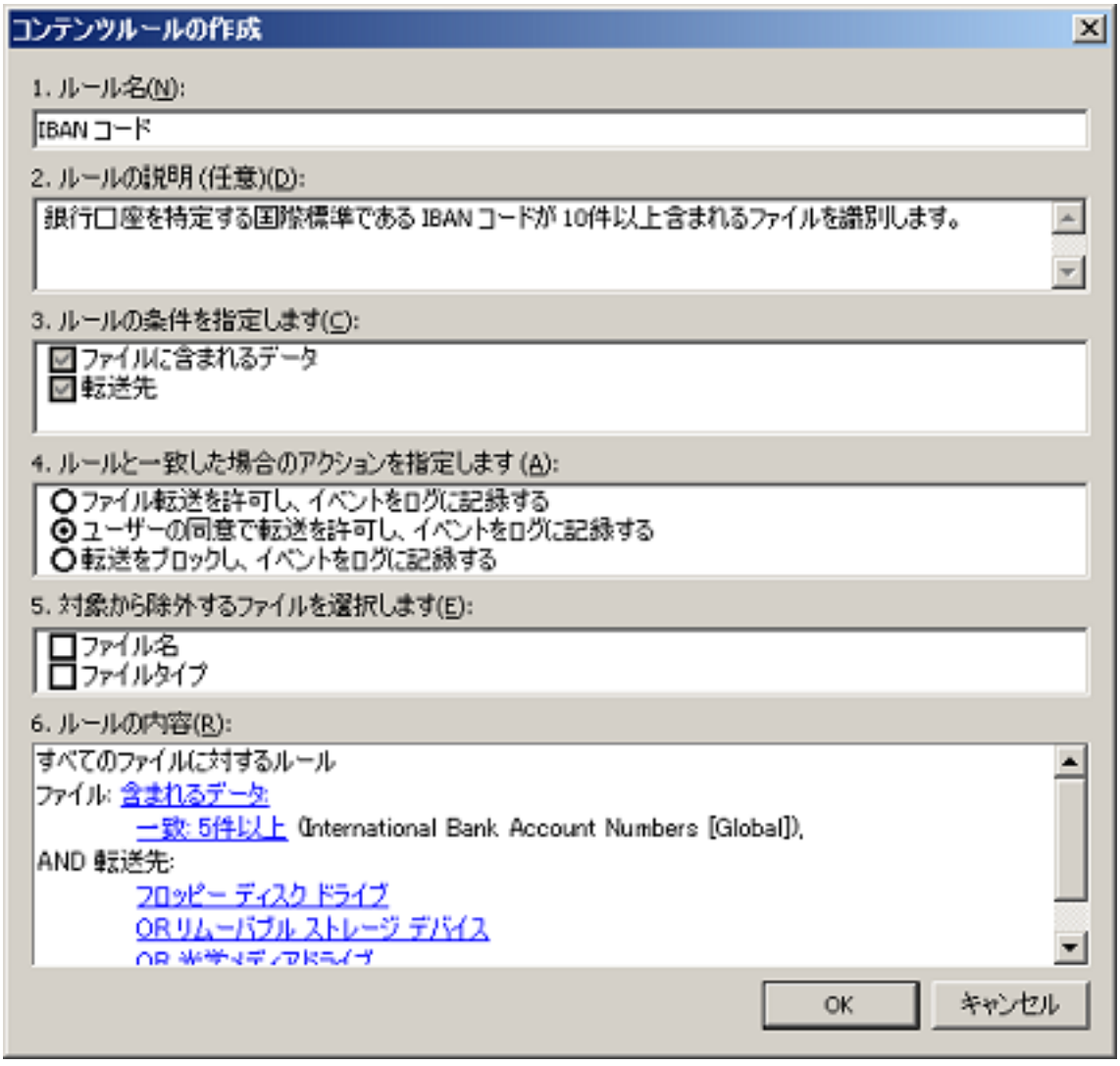
    SophosLabs のコンテンツ コントロール リストを追加する場合は、必要な国それぞれに対するリストを選択します。

ヒント
すべての国に対応する必要がなければ、グローバルのコンテンツ コントロール リストは選択しないでください。対応が必要な国のみに対するコンテンツ コントロール リストを選択してください。このようにすることにより、スキャンの所要時間が大幅に減少するばかりでなく、誤一致のリスクも削減できます。

新しいコンテンツ コントロール リストを作成する場合は、簡単なコンテンツ コントロール リストを作成・編集する (p. 161)、または詳細なコンテンツ コントロール リストを作成・編集する (p. 162)を参照してください。

「**OK**」をクリックします。

12. SophosLabs のコンテンツ コントロール リストに指定されているデータ量を変更する場合は、「**ルールの内容**」欄で、適切な下線付きの「データ量」という値 (「一致: n件以上」など) をクリックします。「**データ量エディタ**」ダイアログボックスで、新しいデータ量を入力します。詳細は、コンテンツ コントロール リストについて (p. 153)を参照してください。
13. 「**ルールの内容**」欄で、残りの下線が付いている項目に対して、条件を選択、または入力します。



「**OK**」をクリックします。

新しいルールが「**データコントロール ルールの管理**」ダイアログボックスに表示されます。

14. ルールをポリシーに追加するには、ルール名の横のチェックボックスを選択し、「**OK**」をクリックします。
    データコントロール ポリシーにルールが追加されます。

データコントロール ポリシーに適用されているルールに一致した際に、当該のユーザーに警告とメッセージを送信するよう設定できます。詳細は、データコントロールの警告やメッセージを設定する (p. 194)を参照してください。

7.4.8 データコントロールのルールをポリシーに追加する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - データコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

データコントロールのルールをポリシーに追加する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのデータコントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**データコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
   「**データコントロール ポリシー**」ダイアログボックスが表示されます。
3. 「**ポリシーのルール**」タブで、「**ルールの追加**」をクリックします。
   「**データコントロール ルールの管理**」ダイアログボックスが表示されます。
4. ポリシーに追加するルールを選択し、「**OK**」をクリックします。

7.4.9 データコントロールのルールをポリシーから削除する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - データコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

データコントロールのルールをポリシーから削除する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのデータコントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**データコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
   「**データコントロール ポリシー**」ダイアログボックスが表示されます。
3. 「**ポリシーのルール**」タブで、削除するルールを選択し、「**ルールの削除**」をクリックします。

7.4.10 データコントロールの対象からファイルやファイルタイプを除外する

ロールベースの管理を利用している場合、データコントロールの対象からファイルを除外するには、「**データコントロール設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

データコントロールの対象から特定のファイルやファイルタイプを除外するには、データコントロールのルールに除外を設定します。

ファイルやファイルタイプをデータコントロールの対象から除外する際は、最も優先度の高いルールに対して除外を設定してください。このようにすることで、最も制限の厳しいアクションを指定できます。

データコントロールの対象からファイルやファイルタイプを除外する方法は次のとおりです。

1. 「**ツール**」メニューで、「**データコントロールの管理**」にカーソルを合わせて「**データコントロールのルール**」をクリックします。
2. 「**データコントロール ルールの管理**」ダイアログボックスで、編集するルールを選択し、「**編集**」をクリックするか、「**ファイルのマッチルールの追加**」ボタンや、「**コンテンツルールの追加**」ボタンをクリックして新しいルールを作成します。
3. ファイルをデータコントロールの対象から除外するには、「**ルールエディタ**」ダイアログボックスの「**対象から除外するファイルを選択します**」欄で、「**ファイル名**」チェックボックスを選択します。
4. 「**ルールの内容**」欄で、該当する下線付きの項目をクリックし、除外するファイル名を指定します。
5. 「**ファイル名を使用した除外の条件**」ダイアログボックスで、「**追加**」をクリックし、対象から除外するファイル名を指定します。

   ワイルドカード文字「*」、および「?」を使用できます。

   ワイルドカード文字「?」は、ファイル名や拡張子の指定のみに使用できます。通常、任意の 1 文字を表します。しかし、ファイル名や拡張子の末尾に使用した場合は、任意の 1文字、または文字のない状態と一致します。たとえば、「file??.txt」は、「file.txt」や「file1.txt」、および「file12.txt」に一致しますが、「file123.txt」には一致しません。

   ワイルドカード文字「*」は、ファイル名や拡張子に対して、[ファイル名].*、または *.[拡張子] という形式だけで使用できます。つまり、「file*.txt」、「file.txt*」、および「file.*txt」などは無効です。
6. 特定のファイルタイプをデータコントロールの対象から除外するには、「**ルールエディタ**」ダイアログボックスの「**対象から除外するファイルを選択します**」欄で、「**ファイルタイプ**」チェックボックスを選択します。
7. 「**ルールの内容**」欄で、該当する下線付きの項目をクリックし、除外するファイルタイプを指定します。
8. 「**ファイルタイプを使用した除外の条件**」ダイアログボックスで、除外するファイルタイプを選択し、「**OK**」をクリックします。

7.4.11 データコントロールのルールをインポート・エクスポートする

ロールベースの管理を利用している場合、データコントロールのルールをインポート、またはエクスポートするには、「**データコントロール設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

データコントロールのルールは、XML ファイルとして Enterprise Console へインポートしたり、Enterprise Console からエクスポートできます。

データコントロールのルールをインポート・エクスポートする方法は次のとおりです。

1. 「**ツール**」メニューで、「**データコントロールの管理**」にカーソルを合わせて「**データコントロールのルール**」をクリックします。
2. 「**データコントロール ルールの管理**」ダイアログボックスで、「**インポート**」または「**エクスポート**」をクリックします。
   - ルールをインポートする場合は、「**インポート**」ダイアログボックスで、インポートするルールを参照し、選択します。そして、「**開く**」をクリックします。
   - ルールをエクスポートする場合は、「**エクスポート**」ダイアログボックスで、ファイルの出力先を参照し、選択します。そして、出力するファイルの名前を入力し、「**保存**」をクリックします。

7.4.12 簡単なコンテンツ コントロール リストを作成・編集する

ロールベースの管理を利用している場合、コンテンツ コントロール リストを作成するには、「**データコントロール設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

コンテンツ コントロール リストの概要は、コンテンツ コントロール リストについて (p. 153)を参照してください。

コンテンツ コントロール リストを作成・編集する方法は次のとおりです。

1. 「**ツール**」メニューで、「**データコントロールの管理**」にカーソルを合わせて「**データコントロールのコンテンツ コントロール リスト**」をクリックします。
2. 「**コンテンツ コントロール リストの管理**」ダイアログボックスで、「**追加**」をクリックして新しいコンテンツ コントロール リストを作成します。または、既存のコンテンツ コントロール リストを選択して「**編集**」をクリックします。
3. 「**コンテンツ コントロール リストの追加**」ダイアログボックスの「**名前**」フィールドに、コンテンツ コントロール リストの名前を入力します。
4. 必要に応じて、「**説明**」フィールドにコンテンツ コントロール リストの説明を入力します。
5. コンテンツ コントロール リストに追加されているタグを追加、または編集する場合は、「**タグ**」フィールドの横にある「**変更**」をクリックします。

   タグを追加すると、コンテンツ コントロール リストの種類や適用地域が識別されます。
6. 「**コンテンツ コントロール リストのタグの編集**」ダイアログボックスの「**利用可能なタグ**」リストから、追加するタグを選択し、「**指定済みタグ**」リストに移動します。「**OK**」をクリックします。
7. 「**コンテンツ マッチの検索**」セクションで、検索条件を選択し (「次のいずれかの用語に一致」、「次のすべての用語に一致」、または「この用語に完全一致」)、ドキュメントに対して検索する用語を空白で区切って入力します。「**OK**」をクリックします。

注

検索では大文字と小文字は区別されません。

簡単なコンテンツ コントロール リストは、引用符を使用した検索に対応していません。完全に一致する用語を検索するには、「この用語に完全一致」条件を選択してください。

さらに複雑な検索条件を設定するには、詳細なコンテンツ コントロール リストを作成・編集する (p. 162)の説明に従って、コンテンツコントロールリストの詳細設定エディタを使用してください。

新しいコンテンツ コントロール リストが「**コンテンツ コントロール リストの管理**」ダイアログボックスに表示されます。

例

検索条件	例	説明
次のいずれかの用語に一致	confidential, secret	「confidential」または「secret」のどちらかを含むドキュメントと一致。
次のすべての用語に一致	project, confidential	「project」と「confidential」の両方を含むドキュメントと一致。
この用語に完全一致	for internal use only	「for internal use only」を含むドキュメントと一致。

次に、コンテンツ コントロール リストをコンテンツルールに追加します。

7.4.13 詳細なコンテンツ コントロール リストを作成・編集する

ロールベースの管理を利用している場合、コンテンツ コントロール リストを作成するには、「**データコントロール設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

コンテンツ コントロール リストの概要は、コンテンツ コントロール リストについて (p. 153)を参照してください。

コンテンツ コントロール リストには、1つ以上の正規表現と 1つの基準スコアを設定できます。設定には詳細設定エディタを使います。

詳細設定エディタを使って、コンテンツ コントロール リストを作成・編集する方法は次のとおりです。

1. 「**ツール**」メニューで、「**データコントロールの管理**」にカーソルを合わせて「**データコントロールのコンテンツ コントロール リスト**」をクリックします。
2. 「**コンテンツ コントロール リストの管理**」ダイアログボックスで、「**追加**」をクリックして新しいコンテンツ コントロール リストを作成します。または、既存のコンテンツ コントロール リストを選択して「**編集**」をクリックします。
3. 「**コンテンツ コントロール リストの追加**」ダイアログボックスの「**名前**」フィールドに、コンテンツ コントロール リストの名前を入力します。
4. 必要に応じて、「**説明**」フィールドにコンテンツ コントロール リストの説明を入力します。
5. コンテンツ コントロール リストに追加されているタグを追加、または編集する場合は、「**タグ**」フィールドの横にある「**変更**」をクリックします。
   タグを追加すると、コンテンツ コントロール リストの種類や適用地域が識別されます。
6. 「**コンテンツ コントロール リストのタグの編集**」ダイアログボックスの「**利用可能なタグ**」リストから、追加するタグを選択し、「**指定済みタグ**」リストに移動します。「**OK**」をクリックします。

7. 「**詳細設定**」ボタンをクリックします。
8. 「**詳細設定**」ペインで、「**作成**」をクリックし、新しい条件式を作成するか、または既存の条件式を選択して「**編集**」をクリックします。
9. 「**コンテンツ コントロール リスト - 詳細設定**」ダイアログボックスで、Perl 5 の正規表現を入力します。

   Perl 5 の正規表現について、詳細は Perl のドキュメントや、http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html (英語) を参照してください。
10. 「**条件式のスコア**」フィールドに、正規表現が一致するたびに、コンテンツ コントロール リストの合計スコアに加算される数値を入力します。
11. 「**最大件数**」フィールドに、合計スコアとして加算される正規表現の最大一致件数を入力します。
    たとえば、条件式のスコアが 5 で、最大件数が 2 の場合、最大 10 がコンテンツ コントロール リストの合計スコアに追加されます。条件式が 3回検出された場合でも、合計スコアに 10 が加算されます。

    「**OK**」をクリックします。
12. コンテンツ コントロール リストに追加する正規表現の数に応じて、ステップ 5～11 を繰り返します。
13. 「**基準スコア**」フィールドに正規表現のマッチ回数を入力します。この値を超えると、コンテンツ コントロール リストが照合されます。

    たとえば、基準スコアが 8 で、3つの条件式 (A、B、および C) を持つコンテンツ コントロール リストに、次のようなスコアと最大件数が設定されているとします。

条件式	スコア	最大件数
条件式 A	5	2
条件式 B	3	1
条件式 C	1	5

    この場合、データコントロールで、条件式 A に 2回マッチした場合、または条件式 A に 1回マッチしてかつ条件式 B にも 1回マッチした場合、 または条件式 B に 1回マッチしてかつ条件式 C にも 5回マッチした場合、コンテンツ コントロール リストが照合されます。

    「**OK**」をクリックします。

新しいコンテンツ コントロール リストが「**コンテンツ コントロール リストの管理**」ダイアログボックスに表示されます。

正規表現の例

(?i)¥b[a-ceghj-npr-tw-z][a-ceghj-npr-tw-z]¥s?¥d{2}¥s?¥d{2}¥s?¥d{2}¥s?[abcd]?¥b

上記の正規表現は、英国の国民保険番号 (例: AA 11 11 11 A) にマッチします。

(?i)	大文字小文字を区別しない。
¥b	単語の境界にマッチする。
[a-ceghj-npr-tw-z]	範囲内の文字列 (この例では、A～C E G H J～NP R～T W～Z) のいずれか 1文字にマッチする。

?	直前の文字が 0個または 1個ある場合にマッチする。
¥s?	0個または 1個の空白文字にマッチする。
¥d{2}	2桁の数値にマッチする。
[abcd]	[ ] の中の任意の1文字にマッチする (この例では、A、B、C、D のいずれか)。

次に、コンテンツ コントロール リストをコンテンツルールに追加します。

7.4.14 コンテンツ コントロール リストをインポート・エクスポートする

ロールベースの管理を利用している場合、コンテンツ コントロール リストをインポート、またはエクスポートするには、「**データコントロール設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

コンテンツ コントロール リストは、XML ファイルとして Enterprise Console へインポートしたり、Enterprise Console からエクスポートできます。コンテンツ コントロール リストに対応している他のソフォス製品でもリストを使用できます。

注
SophosLabs コンテンツ コントロール リストをエクスポートすることはできません。

コンテンツ コントロール リストをインポート・エクスポートする方法は次のとおりです。

1. 「**ツール**」メニューで、「**データコントロールの管理**」にカーソルを合わせて「**データコントロールのコンテンツ コントロール リスト**」をクリックします。
2. 「**コンテンツ コントロール リストの管理**」ダイアログボックスで、「**インポート**」または「**エクスポート**」をクリックします。
   - コンテンツ コントロール リストをインポートする場合は、「**インポート**」ダイアログボックスで、インポートするリストを参照し、選択します。そして、「**開く**」をクリックします。
   - コンテンツ コントロール リストをエクスポートする場合は、「**エクスポート**」ダイアログボックスで、ファイルの出力先を参照し、選択します。そして、出力するファイルの名前を入力し、「**保存**」をクリックします。

7.5 デバイスコントロール ポリシー

注
この機能はすべてのライセンスには含まれていません。利用するには追加購入が必要となります。詳細は、http://www.sophos.com/ja-jp/products/complete/comparison.aspxを参照してください。

重要
ソフォスのデバイスコントロール機能は、他社製デバイスコントロール ソフトがインストール済みの環境にはインストールしないでください。

デバイスコントロール機能では、各コンピュータにおける、認証されていない外付けのハードディスク機器、リムーバブル ストレージ メディア、および無線接続機器の使用を防止することができます。これによって、事故などによるデータ流出リスクを大幅に削減することができ、また、ユーザーによる社内ネットワークへのソフトウェアの持ち込みを制限できます。

また、リムーバブル ストレージ デバイス、光学ディスクドライブ、およびフロッピーディスクドライブに対して、読み取り専用の制限を設けることもできます。

また、デバイスコントロール機能では、企業ネットワークと外部ネットワーク間におけるブリッジ接続のリスクを大幅に削減できます。ワイヤレス接続、モデム接続のどちらでも、「**ブリッジ接続をブロックする**」モードを利用できます。この動作モードは、エンドポイントが物理的なネットワーク (通常、イーサネットで接続) に接続した際に、ワイヤレスアダプタかモデムのどちらかが無効になることで作動します。エンドポイントを物理的なネットワークから切り離すと、シームレスにワイヤレスアダプタやモデムは再度有効になります。

デフォルトで、デバイス コントロールは無効になっています。すべてのデバイスが許可されています。

はじめてデバイスコントロール機能を有効にする際は、次のように設定することを推奨します。

- 使用をコントロールするデバイスの種類を選択する。
- デバイスをブロックせずに検出する。
- デバイスコントロールのイベントを使って、どの種類のデバイスをブロックし、どの種類のデバイスを対象から除外するか (必要な場合) を決定する。
- デバイスを検知・ブロックするか、またはストレージデバイスに対して読み取り専用の制限を設ける。

デバイスコントロールの推奨設定について、詳細は「Sophos Enterprise Console ポリシー設定ガイド」を参照してください。

注
ロールベースの管理を利用している場合は次の点に注意してください。

- デバイスコントロール ポリシーを設定するには、「**ポリシー設定 - デバイスコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

7.5.1 デバイスコントロールのイベントについて

デバイスコントロールのイベント (リムーバブル ストレージ デバイスがブロックされたなど) が発生すると、Enterprise Console に情報が送信されます。送信されたイベントは、「**デバイスコントロール - イベントビューア**」で表示できます。

注
「読み取り専用」に設定した光学ディスクドライブのイベントは Enterprise Console に送信されず、ローカルディスクにもログ出力されません。これにより、不要なイベントレポートの生成を防止できます。

「**デバイスコントロール - イベントビューア**」ダイアログボックスでは、必要な情報をフィルタで抽出できます。また、デバイスコントロールのイベントの一覧をファイルに出力できます。詳細は、デバイスコントロールのイベントについて (p. 165)、およびイベントの一覧をファイルに出力する (p. 208)を参照してください。

また、デバイスコントロールのイベント設定ページで、デバイスコントロールのポリシーに対して、特定のデバイスやデバイスモデルを対象から除外するよう設定できます。デバイスの除外の詳細は、デバイスを特定のポリシーの対象から除外する (p. 170)、またはデバイスをすべてのポリシーの対象から除外する (p. 169)を参照してください。

過去 1週間で、デバイスコントロールのイベントが、しきい値を超えて発生したコンピュータの台数は、ダッシュボードに表示されます。しきい値の設定方法については、ダッシュボードを環境設定する (p. 48)を参照してください。

また、デバイスコントロールのイベントが発生した場合に、特定の受信者に警告を送信するよう設定できます。詳細は、デバイスコントロールの警告やメッセージを設定する (p. 195)を参照してください。

7.5.2 制御可能なデバイスの種類

デバイスコントロールでブロックできるデバイスは、ストレージデバイス、ネットワークデバイス、短距離無線通信デバイス、メディアデバイスです。

ストレージデバイス

- リムーバブル ストレージ デバイス (USB フラッシュドライブ、PC カードリーダ、外付けハードディスクドライブなど)
- 光学メディアドライブ (CD-ROM/DVD/Blu-ray ドライブ)
- フロッピーディスクドライブ
- セキュリティ搭載リムーバブル ストレージ デバイス (ハードウェア暗号化機能搭載 USB メモリなど)

サポートされているセキュリティ搭載リムーバブル ストレージ デバイスの一覧は、ソフォスのサポートデータベースの文章 63102 を参照してください。

ヒント
セキュアなリムーバブルストレージのカテゴリを使うと、他のリムーバブル ストレージ デバイスをブロックしつつ、カテゴリに該当するセキュアなリムーバブル ストレージ デバイスの使用を簡単に許可できます。

ネットワークデバイス

- モデム
- ワイヤレス機器 (Wi-Fi インターフェース、802.11 規格)

また、ネットワークインターフェースに対して、「**ブリッジ接続をブロックする**」モードを選択すると、企業ネットワークと外部ネットワーク間におけるブリッジ接続のリスクを大幅に削減できます。この動作モードは、エンドポイントが物理的なネットワーク (通常、イーサネットで接続) に接続した際に、ワイヤレスアダプタかモデムのどちらかが無効になることで作動します。エンドポイントを物理的なネットワークから切り離すと、シームレスにワイヤレスアダプタやモデムは再度有効になります。

短距離無線通信デバイス

- Bluetooth インターフェース

- 赤外線 (IrDA 赤外線インターフェース)

デバイスコントロールでは、内蔵型と外付け両方のデバイス/インターフェースがブロックされます。たとえば、Bluetooth インターフェースをブロックするポリシーは、次のどちらのインターフェースもブロックします。

- コンピュータに内蔵されている Bluetooth インターフェース
- コンピュータに接続されている USB ベースの Bluetooth アダプタ

メディアデバイス

- MTP/PTP

  MTP (メディア転送プロトコル) や PTP (画像転送プロトコル) を使用してコンピュータに接続する、携帯電話、タブレット端末、デジタルカメラ、メディアプレーヤー、およびその他のデバイスが含まれます。

7.5.3 コントロールするデバイスの種類を選択する

ロールベースの管理を利用している場合は次の点に注意してください。

- デバイスコントロール ポリシーを編集するには、「**ポリシー設定 - デバイスコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

重要
Wi-Fi 経由で集中管理しているコンピュータがある場合、当該のコンピュータにおける Wi-Fi 接続はブロックしないでください。

1. 設定するコンピュータのグループ (複数可) に、どのデバイスコントロール ポリシーが適用されているか確認してください。

   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**デバイスコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**デバイスコントロール ポリシー**」ダイアログボックスの「**環境設定**」タブで、「**ストレージ**」項目から使用をコントロールするストレージデバイスを選択します。
4. 「タイプ」の隣の「**ステータス**」カラムをクリックし、表示されるドロップダウン矢印をクリックします。許可するアクセスの種類を選択します。

   デフォルトで、デバイスにはフルアクセスが許可されています。リムーバブル ストレージ デバイス、光学ディスクドライブ、およびフロッピーディスクドライブについては、「ブロック」または「読み取り専用」に変更できます。セキュアなリムーバブル ストレージ デバイスについては、「ブロック」に変更できます。
5. 「**ネットワーク**」の項目から、ブロックするネットワークデバイスの種類を選択します。
6. ネットワークデバイス タイプの隣の「**ステータス**」カラムをクリックし、表示されるドロップダウン矢印をクリックします。
   - ブロックするデバイスタイプに対して、「ブロック」を選択します。
   - 企業ネットワークと外部ネットワーク間のブリッジ接続を阻止するには、「ブリッジ接続をブロックする」を選択します。このデバイスタイプは、エンドポイントが物理的なネットワーク

(通常、イーサネットで接続) に接続した際にブロックされます。エンドポイントを物理的なネットワークから切り離すと、同デバイスタイプは再度有効になります。

7. 「**短距離無線通信デバイス**」の項目から、ブロックする短距離無線通信デバイスの種類を選択します。デバイスタイプの隣りの「**ステータス**」カラムで、「ブロック」を選択します。

   「**OK**」をクリックします。

8. 携帯電話、タブレット端末、デジタルカメラ、メディアプレーヤーなど、MTP (メディア転送プロトコル) や PTP (画像転送プロトコル) を使用してコンピュータに接続するメディアデバイスをブロックするには、「**メディアデバイス**」で「**MTP/PTP**」を選択してください。「**ステータス**」カラムで、「ブロック」を選択します。

7.5.4 デバイスをブロックせずに検出する

ロールベースの管理を利用している場合は次の点に注意してください。

- デバイスコントロール ポリシーを編集するには、「**ポリシー設定 - デバイスコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デバイスはブロックすることなく検出できます。このオプションを利用すると、デバイスのブロックを有効にする前に、デバイスを検出し、必要なものをデバイスコントロールの対象から除外できるので便利です。

デバイスをブロックせずに検出するには、デバイスコントロール ポリシー内でデバイスコントロールを有効に設定し、検出のみモードを有効にします。検出するデバイスのステータスを「ブロック」に変更します。これにより、ポリシーに反する動作があった際に、各エンドポイントコンピュータで使用されるデバイスをブロックすることなく、デバイスのイベントが生成されます。

デバイスコントロールのイベントの詳細は、デバイスコントロールのイベントについて (p. 165)を参照してください。

デバイスをブロックせずに検出する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのデバイスコントロール ポリシーが適用されているか確認してください。

   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。

2. 「**ポリシー**」ペインで、「**デバイスコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**デバイスコントロール ポリシー**」ダイアログボックスの「**環境設定**」タブで、「**デバイスコントロールを有効にする**」を選択します。
4. 「**デバイスを検出するが、ブロックしない**」を選択します。
5. まだ未設定の場合は、検出するデバイスのステータスを「ブロック」に変更します。(詳細は、コントロールするデバイスの種類を選択する (p. 167)を参照してください。)

   「**OK**」をクリックします。

7.5.5 デバイスを検出・ブロックする

ロールベースの管理を利用している場合は次の点に注意してください。

- デバイスコントロール ポリシーを編集するには、「**ポリシー設定 - デバイスコントロール**」権限が必要です。

- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

1. 設定するコンピュータのグループ (複数可) に、どのデバイスコントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**デバイスコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**デバイスコントロール ポリシー**」ダイアログボックスの「**環境設定**」タブで、「**デバイスコントロールを有効にする**」チェックボックスを選択します。
4. 「**デバイスを検出するが、ブロックしない**」チェックボックスの選択を外します。
5. まだ未設定の場合は、ブロックするデバイスのステータスを「ブロック」に変更します。(詳細は、管理対象アプリケーションを選択する (p. 147)を参照してください。)
   「**OK**」をクリックします。

7.5.6 デバイスをすべてのポリシーの対象から除外する

ロールベースの管理を利用している場合は次の点に注意してください。

- デバイスコントロール ポリシーを編集するには、「**ポリシー設定 - デバイスコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトのポリシーを含む、すべてのポリシーの対象からデバイスを除外できます。この除外設定は、以後、作成するすべてのポリシーに適用されます。

デバイスは個別に除外するか (「このデバイスのみ」)、または特定のデバイスモデルを除外できます (「このモデル ID のデバイスすべて」)。1台のデバイスに対して、除外の設定は、必ず、個別かモデル ID 別か、どちらか 1つで設定してください。両方設定した場合、個別のデバイスの設定が優先されてしまいます。

デバイスをすべてのデバイスコントロール ポリシーの対象から除外する方法は次のとおりです。

1. 「**イベント**」メニューの「**デバイスコントロールのイベント**」をクリックします。
   「**デバイスコントロール - イベントビューア**」ダイアログボックスが表示されます。
2. 特定のイベントだけを表示する場合は、「**検索の条件**」ペインで、適宜フィルタを設定します。そして、「**検索**」をクリックしてイベントを表示します。
   詳細は、デバイスコントロールのイベントについて (p. 165)を参照してください。
3. ポリシーから除外するデバイスのエントリを選択し、「**デバイスの除外**」をクリックします。
   「**デバイスの除外**」ダイアログボックスが表示されます。「**デバイスの詳細**」に、デバイスのタイプ、モデル、モデル ID、およびデバイス ID が表示されます。「**除外の詳細**」の「**スコープ**」の下に、「すべてのポリシー」と表示されます。

注
除外の対象にしたいデバイス (エンドポイントコンピュータの内蔵型 CD/DVD ドライブなど) のイベントがない場合は、当該のデバイスのあるコンピュータに移動し、「デバイス マネージャ」でデバイスを有効にします。(「デバイス マネージャ」を開くには、「**マイ コンピュータ**」を右クリックし、「**管理**」をクリックします。そして、「**デバイス マネージャ**」をクリックします。)これにより、「ブロック」イベントが発生し、「**デバイスコントロール - イベントビューア**」ダイアログボックスに表示されます。このステップのはじめに説明した方法で、デバイスを除外します。

4. このデバイスのみ除外するか、または、このモデル ID のデバイスすべてを除外するか選択します。
5. デバイスに対して、フルアクセス、または読み取り専用のアクセスを許可します。
6. 必要に応じて、「**コメント**」フィールドにコメントを入力します。たとえば、除外設定の申請者名などを入力できます。
7. 「**OK**」をクリックします。

7.5.7 デバイスを特定のポリシーの対象から除外する

ロールベースの管理を利用している場合は次の点に注意してください。

- デバイスコントロール ポリシーを編集するには、「**ポリシー設定 - デバイスコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

特定のデバイスをデバイスコントロールポリシーの対象から除外できます。

デバイスは個別に除外するか (「このデバイスのみ」)、または特定のデバイスモデルを除外できます (「このモデル ID のデバイスすべて」)。1台のデバイスに対して、除外の設定は、必ず、個別かモデル ID 別か、どちらか 1つで設定してください。両方設定した場合、個別のデバイスの設定が優先されてしまいます。

デバイスをポリシーの対象から除外する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのデバイスコントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**デバイスコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**デバイスコントロール ポリシー**」ダイアログボックスの「**環境設定**」タブで、「**除外の追加**」をクリックします。
   「**デバイスコントロール - イベントビューア**」ダイアログボックスが表示されます。
4. 特定のイベントだけを表示する場合は、「**検索の条件**」ペインで、適宜フィルタを設定します。そして、「**検索**」をクリックしてイベントを表示します。
   詳細は、デバイスコントロールのイベントについて (p. 165)を参照してください。
5. ポリシーから除外するデバイスのエントリを選択し、「**デバイスの除外**」をクリックします。
   「**デバイスの除外**」ダイアログボックスが表示されます。「**デバイスの詳細**」に、デバイスのタイプ、モデル、モデル ID、およびデバイス ID が表示されます。「**除外の詳細**」の「**スコープ**」の下に、「このポリシーのみ」と表示されます。

注
除外の対象にしたいデバイス (エンドポイントコンピュータの内蔵型 CD/DVD ドライブなど) のイベントがない場合は、当該のデバイスのあるコンピュータに移動し、「デバイス マネージャ」でデバイスを有効にします。(「デバイス マネージャ」を開くには、「**マイ コンピュータ**」を右クリックし、「**管理**」をクリックします。そして、「**デバイス マネージャ**」をクリックします。)これにより、「ブロック」イベントが発生し、「**デバイスコントロール - イベントビューア**」ダイアログボックスに表示されます。このステップのはじめに説明した方法で、デバイスを除外します。

6. このデバイスのみ除外するか、または、このモデル ID のデバイスすべてを除外するか選択します。
7. デバイスに対して、フルアクセス、または読み取り専用のアクセスを許可します。
8. 必要に応じて、「**コメント**」フィールドにコメントを入力します。たとえば、除外設定の申請者名などを入力できます。
9. 「**OK**」をクリックします。

7.5.8 管理対象外のデバイスのリストを表示/編集する

ロールベースの管理を利用している場合は次の点に注意してください。

- デバイスコントロール ポリシーを編集するには、「**ポリシー設定 - デバイスコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

管理対象外のデバイスのリストを表示/編集する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのデバイスコントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**デバイスコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**デバイスコントロール ポリシー**」ダイアログボックスの「**環境設定**」タブで、除外を表示する管理対象外のドライブの種類 (例: 光学ドライブなど) を選択します。「**除外の表示**」をクリックします。
   「**<デバイスタイプ> の除外**」ダイアログボックスが表示されます。除外の対象が特定のモデル ID のデバイスすべての場合は、「**デバイス ID**」フィールドには何も表示されません。
4. 管理対象デバイスのリストを編集する場合は、次のいずれかの手順を実行します。
   - 除外を追加する場合は、「**追加**」をクリックします。詳細は、デバイスを特定のポリシーの対象から除外する (p. 170)を参照してください。
   - 除外を編集する場合は、編集する除外を選択し、「**編集**」をクリックします。「**デバイスの除外**」ダイアログの設定を適宜編集します。
   - 除外を削除する場合は、除外項目を選択し、「**削除**」をクリックします。
     これにより、編集中のポリシーから当該の除外項目が削除されます。他のポリシーからも当該の除外項目を削除する場合は、各ポリシーに対して同じステップを繰り返してください。

7.6 タンパー プロテクション ポリシー

タンパー プロテクションは、未認証のユーザー (ローカルアドミニストレータや専門知識のないユーザーなど) や既知のマルウェアが、ソフォスのセキュリティソフトをアンインストールしたり、Sophos Endpoint Security and Control の GUI を通じて無効に設定することを防止する機能です。

注
この機能は詳しい専門知識を持つユーザーから製品を保護するものではありません。また、検出を避けるために OS を妨害するマルウェアから製品を保護するものでもありません。このタイプのマルウェアは、脅威検索や疑わしい動作検索のみで検出されます。(詳細は、ウイルス対策および HIPS ポリシー (p. 80)を参照してください。)

タンパー プロテクションを有効にし、タンパー プロテクションのパスワードを作成すると、パスワードが与えられていない SophosAdministrator グループのメンバーは次の操作ができなくなります。

- Sophos Endpoint Security and Control でオンアクセス検索や疑わしい動作の検知を再設定する。
- タンパー プロテクションを無効にする。
- Sophos Endpoint Security and Control のコンポーネント (Sophos Anti-Virus、Sophos Client Firewall、Sophos AutoUpdate、Sophos Remote Management System) をアンインストールする。

SophosAdministrator グループのメンバーに上記のタスクの実行を許可するには、タンパー プロテクションのパスワードを通知する必要があります。ユーザーはまずパスワード認証を行います。

SophosUser および SophosPowerUser グループのメンバーは、タンパー プロテクション機能による影響を受けません。タンパー プロテクションを有効にした場合、これらのユーザーは、タンパー プロテクションのパスワードを入力せずに、通常、実行を許可されているタスクすべてを実行できます。

注
ロールベースの管理を利用している場合は次の点に注意してください。

- タンパー プロテクション ポリシーを設定するには、「**ポリシー設定 - タンパー プロテクション**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

タンパー プロテクションのイベント

たとえば、未認証のユーザーがエンドポイントコンピュータから Sophos Anti-Virust をアンインストールしようとした操作をブロックするなど、タンパー プロテクションのイベントが発生すると、イベントログに記録されます。記録されたログは Enterprise Console で表示できます。詳細は、タンパー プロテクションのイベントを表示する (p. 202)を参照してください。

タンパー プロテクションのイベントには次の 2種類があります。

- タンパー プロテクションの認証に成功したときに記録されるイベント。認証済みのユーザーの名前と認証した日時が表示されます。
- ソフォス製品を改変しようとする操作が失敗したときに記録されるイベント。当該のソフォス製品またはコンポーネントの名前、発生日時、操作を行ったユーザーの名前が表示されます。

7.6.1 タンパー プロテクションを有効/無効に切り替える

ロールベースの管理を利用している場合は次の点に注意してください。

- タンパー プロテクション ポリシーを設定するには、「**ポリシー設定 - タンパー プロテクション**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

タンパー プロテクションを有効/無効に切り替える方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのタンパー プロテクション ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**タンパー プロテクション**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**タンパー プロテクション ポリシー**」ダイアログボックスで、「**タンパー プロテクションを有効にする**」チェックボックスを選択するか、または選択を外します。
   はじめてタンパー プロテクション機能を有効にする際は、「**パスワードボックス**」で「**セット**」をクリックします。「**タンパー プロテクションのパスワード**」ダイアログボックスに、パスワードを入力し、確認入力します。

ヒント
パスワードは、大文字、小文字、数字を組み合わせ、8文字以上指定することを推奨します。

7.6.2 タンパー プロテクションのパスワードを変更する

タンパー プロテクションのパスワードを変更する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのタンパー プロテクション ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**タンパー プロテクション**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**タンパー プロテクション ポリシー**」ダイアログボックスで、「**パスワード**」ボックスの「**変更**」をクリックします。「**タンパー プロテクションのパスワード**」ダイアログボックスに、パスワードを入力し、確認入力します。

ヒント
パスワードは、大文字、小文字、数字を組み合わせ、8文字以上指定する必要があります。

7.6.3 拡張タンパープロテクションについて

拡張タンパープロテクションは、タンパー プロテクションを基にした機能です。拡張タンパープロテクションを有効にすると、Sophos Anti-Virus、Sophos AutoUpdate、Sophos Management Communication System、Sophos Remote Management System および Sophos Endpoint Defense で、次の操作がブロックされます。

- 「サービス」画面でサービスを停止する
- 「タスクマネージャー」画面でサービスを終了する
- 「サービス」画面でサービスの設定を変更する
- コマンドラインで、サービスを停止したり、サービスの設定を編集したりする
- アンインストールする
- 再インストールする
- 「タスクマネージャー」画面でプロセスを終了する
- 保護対象ファイルまたはフォルダを削除/変更する
- 保護対象レジストリキーを削除/変更する

重要
拡張タンパープロテクションを有効にするには、タンパー プロテクションを有効にする必要があります。タンパー プロテクションを無効にすると、拡張タンパープロテクションは自動的に無効化されます。

7.6.4 拡張タンパープロテクションの設定

1. 「**ポリシー**」ペインで、「**タンパー プロテクション**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
2. 「**タンパー プロテクション ポリシー**」ダイアログボックスで、「**タンパー プロテクションを有効にする**」チェックボックスが選択されていることを確認してから、「**拡張タンパープロテクションを有効にする**」チェックボックスを選択します。
3. 新規インストールまたはアップグレードの場合、「**タンパー プロテクション ポリシー**」ダイアログボックスで、「**パスワード**」ボックスの下にある「**設定**」をクリックします。

   タンパー プロテクションが既に有効化されている場合は、「**パスワード**」ボックスの下にある「**変更**」をクリックします。「**タンパー プロテクションのパスワード**」ダイアログボックスで、パスワードを入力し、確認入力します。

   注
   タンパー プロテクションと拡張タンパー プロテクションでは、同じパスワードが使用されます。拡張タンパープロテクションを有効にすると、タンパー プロテクションは上書きされます。このため、タンパー プロテクションのパスワードを設定済みの場合は、それを変更する必要があります。

   各ポリシーに対して、異なるパスワードを設定することを推奨します。

7.7 パッチ ポリシー

注
この機能はすべてのライセンスには含まれていません。利用するには追加購入が必要となります。詳細は、http://www.sophos.com/ja-jp/products/complete/comparison.aspxを参照してください。

Enterprise Console では、お使いのコンピュータに最新のセキュリティパッチが適用されているかどうかをチェックできます。

SophosLabs が定義する緊急度から、最も深刻なセキュリティパッチがどれであるかがわかるため、緊急性の高い問題にすばやく対処できます。最新の攻撃情報をもとに算出しているため、SophosLabs が指定するパッチの緊急度は他のベンダーによる深刻度評価と異なる場合があります。

パッチ評価機能を利用する前に、ネットワーク上のコンピュータにパッチエージェントをインストールする必要があります。パッチエージェントは、パッチの評価を実行してその結果を Enterprise Console に送信します。インストールには「**コンピュータの保護 ウィザード**」を使用します。詳細は、コンピュータを自動保護する (p. 45)を参照してください。

ここでの説明はパッチエージェントがインストール済みであることを想定しています。

注
ロールベースの管理を利用している場合は次の点に注意してください。

- パッチポリシーを設定するには、「**ポリシー設定 - パッチ**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

7.7.1 パッチ評価の仕組み

パッチ評価はデフォルトのポリシーで無効に設定されています。パッチ評価を有効化すると、コンピュータで評価が開始されます。これには数分かかることがあります。以後、ポリシーで設定されている頻度に基づいて (デフォルトで一日一回) 評価が行われます。

注
Enterprise Console がソフォスからパッチの評価データを一度もダウンロードしない状態でコンピュータの評価を実行した場合、パッチ評価のイベントビューアに結果は表示されません。ダウンロードには数時間かかることがあります。ダウンロードが完了したかどうかを確認するには、「**イベント - パッチ評価のイベント**」の「**パッチ情報**」フィールドを参照します。

何らかの理由で、Enterprise Console からパッチエージェントが更新されなかった場合は、前回ダウンロードしたパッチ検出データに基づいてコンピュータの評価が実施されます。

セキュリティパッチが適用されているかどうかの評価は、コンピュータにインストール済みのソフトウェアのみに対して実施されます。既存のパッチを置き換える新たなパッチがリリースされると、古い方のパッチが適用されているかどうかはチェックされなくなります。新しいパッチのみに対して評価が実施されます。

パッチの置き換えとは？

過去にリリースされたパッチはベンダーによって置き換えられることがありますが、この新しいパッチを「置き換え後のパッチ」といいます。置き換えられる古いパッチは、「置き換え前のパッチ」といいます。

コンピュータを最新の状態に保つには、置き換え後のパッチを適用することを推奨します。

例: 「virusX」というウイルスに対する修正を含むパッチ「P01」が、「P02」に置きかえられた場合、「P02」をインストールすることを推奨します。

7.7.2 パッチ評価のイベントについて

パッチ評価のイベント (パッチがインストールされていないコンピュータの検出など) が発生すると、Enterprise Console にイベントの情報が送信されます。送信されたイベントは、「**パッチ評価 - イベントビューア**」で表示できます。

「**パッチ評価 - イベントビューア**」で、フィルタを使用して確認したいイベントのみを表示することができます。またパッチ評価のイベントのリストをファイルに出力することもできます。詳細は、パッチ評価のイベント (p. 202)、およびイベントの一覧をファイルに出力する (p. 208)を参照してください。

7.7.3 パッチ評価を有効/無効に切り替える

ロールベースの管理を利用している場合は次の点に注意してください。

- パッチポリシーを設定するには、「**ポリシー設定 - パッチ**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

パッチ評価を有効/無効に切り替える方法は次のとおりです。

1. 設定するコンピュータのグループに、どのパッチポリシーが指定されているかを確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**パッチ**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**パッチポリシー**」ダイアログボックスで、「**パッチ評価を有効にする**」チェックボックスを選択から外します。そして、「**OK**」をクリックします。

7.7.4 パッチ評価の頻度を選択する

ロールベースの管理を利用している場合は次の点に注意してください。

- パッチポリシーを設定するには、「**ポリシー設定 - パッチ**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

パッチ評価の頻度を選択する方法は次のとおりです。

1. 設定するコンピュータのグループに、どのパッチポリシーが指定されているかを確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**パッチ**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**パッチポリシー**」ダイアログボックスで、「**未適用パッチの評価**」フィールドのドロップダウン矢印をクリックして適切な評価頻度を選択します。「**OK**」をクリックします。
   ここで選択した頻度で評価を実施するには、ポリシーでパッチ評価を有効に設定する必要があります。

7.8 Web コントロール ポリシー

注
この機能はすべてのライセンスには含まれていません。利用するには追加購入が必要となります。詳細は、http://www.sophos.com/ja-jp/products/complete/comparison.aspxを参照してください。

Enterprise Console では、デフォルトで、Web コントロール ポリシーは無効になっています。「**Web コントロールを有効にする**」を選択すると、次のいずれか 1つのポリシーオプションを指定できます。

- **不適切な Web サイトのコントロール**: この基本的な Web コントロールのオプションでは、14種類の基本的なカテゴリに基づいて設定を行うことができます。このオプションは、ユーザーがアクセスすることで、組織が法的責任を問われる可能性がある Web サイトに対して指定できます。詳細は、不適切な Web サイトのコントロール (p. 178)を参照してください。
- **高度な Web コントロール**: 全機能に対応した包括的なポリシー (50種類以上の Web サイトカテゴリに対応) を適用します。このオプションを利用するには、Sophos Web Appliance、Sophos Management Appliance (共に日本では未提供)、または Sophos UTM アプライアンス (バージョン 9.2 以降) が必要です。これらのアプライアンスと連携してエンドポイントとの同期を行い、ポリシーのアップデートを配信したり、Web の活動履歴を収集します。詳細は、高度な Web コントロール (p. 182)を参照してください。

「不適切な Web サイトのコントロール」オプションを使用する場合、既存の Web コントロール ポリシーを編集するか、新しいポリシーを作成することができます。詳細は、ポリシーを作成する (p. 31)を参照してください。各カテゴリをそれぞれ「ブロック」、「警告」または「許可」に指定できます。Web コントロールのステータスと Web のイベントは、Enterprise Consoleに表示されます。Web イベントの詳細は、Web のイベントを表示する (p. 205)を参照してください。

「高度な Web コントロール」ポリシーを使用している場合、Enterprise Console では、詳細な Web コントロール ポリシーを設定する Web Appliance、UTM アプライアンス、または Management Appliance のロケーション情報、およびアプライアンスと Enterprise Console との間でセキュア通信を行うために共有鍵が必要となります。「高度な Web コントロール」ポリシーが選択されると、ほとんどのレポート・監視はアプライアンスで行われるようになります。ただし、Sophos Endpoint Security and Control のライブ URL フィルタリング (Web Protection (p. 101)) 機能でスキャン・評価された Web サイトは Enterprise Console に Web のイベントとして表示されます。

Web コントロールについての詳細は、「エンドポイントにおける Web コントロール概要ガイド」を参照してください。

注
ロールベースの管理を利用している場合は次の点に注意してください。

- Web コントロール ポリシーを編集するには、「**ポリシー設定 - Web コントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

7.8.1 不適切な Web サイトのコントロール

注
この機能はすべてのライセンスには含まれていません。利用するには追加購入が必要となります。詳細は、http://www.sophos.com/ja-jp/products/complete/comparison.aspxを参照してください。

基本的な Web サイトのコントロールを使用すると、14種類の Web サイトのカテゴリに基づいて、ユーザーの Web アクセスをコントロールできます。各カテゴリに対してデフォルトのアクションが指定されていますが (Web サイトのカテゴリについて (p. 179)を参照)、必要に応じて別のアクション (Web サイトのカテゴリに対する操作を選択する (p. 181)を参照) を選択できます。

制限付き Web サイトへのユーザーアクセスをブロックすることができます。イベントが作成され、ユーザーに対して表示され、Enterprise Console に送信されます。

また、ユーザーが制限付きサイトにアクセスすると、警告が表示されるように設定することもできます。ユーザーが操作を続行しない場合でも、警告イベントが作成されます。警告が表示されたにも関わらず、ユーザーが操作を続行してサイトを表示すると、イベントがさらにもう 1つ作成され Enterprise Console に送信されます。

注
対応している全種類の Web ブラウザで、HTTP サイトと HTTPS サイトの両方がコントロールされますが、URL が HTTP か HTTPS によってユーザー通知の方法は異なります。HTTP サイトの場合、「ブロック」または「警告」に指定されたカテゴリに属するサイトにアクセスすると、ユーザーに通知ページが表示されます。HTTPS サイトの場合、サイトが「ブロック」されている場合のみユーザーに通知が表示され、通知は、バルーン ヒントとして Windows システムトレイに表示されます。「警告」に指定された HTTPS サイトにアクセスしても、ユーザー通知が行われることはなく、ログにも記録されません。代わりに、要求したページへのユーザーアクセスの続行が許可され、そのイベントは、Enterprise Console で「続行」されたアクションとしてログに記録されます。

特定の Web サイトのカテゴリに対して「許可」を選択した場合、例外 Web サイトが指定されていない限り、ユーザーはそのカテゴリに属する Web サイトすべてにアクセスすることができます。「**不適切な Web サイトのコントロール**」を選択している場合、「許可」に指定されたサイトへのアクセスはログに記録されません。

注
なお、許可された Web サイトも、Sophos Endpoint Security and Control のライブ URL フィルタリング (Web Protection) 機能でスキャン・評価されます。

不適切な Web サイトのコントロールを有効にする

Enterprise Console で Web コントロールを有効にし、不適切な Web サイトのコントロール ポリシーを使用するには、次の手順を実行してください。

注
ロールベースの管理を利用している場合は次の点に注意してください。

- Web コントロール ポリシーを編集するには、「**ポリシー設定 - Web コントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

不適切な Web サイトのコントロールを有効にする方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どの Web コントロール ポリシーが適用されているか確認してください。詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**Web コントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
   「**Web コントロール ポリシー**」ダイアログボックスが表示されます。
3. 「**全般**」タブで、「**Web コントロールを有効にする**」を選択します。
   「**不適切な Web サイトのコントロール**」ポリシーが表示されます。14種類の各カテゴリに対してデフォルトのアクションが指定されていますが、別のアクションを指定することもできます。詳細は、Web サイトのカテゴリに対する操作を選択する (p. 181)を参照してください。

Web サイトのカテゴリについて

「**不適切な Web サイトのコントロール**」を選択し、14種類の Web サイトのカテゴリを設定して、Web ブラウザ経由でユーザーがアクセスできるインターネットのコンテンツをコントロールすることができます。詳細は、不適切な Web サイトのコントロール (p. 178)を参照してください。

以下で説明する Web サイトのカテゴリがコントロールの対象となります。各カテゴリに対するデフォルトの操作は、括弧内を参照してください。各カテゴリに対して、「**ブロック**」、「**警告**」または「**許可**」を指定できます。「**許可**」を選択すると、そのカテゴリに属するすべての Web サイトに対するアクセスをユーザーに許可します。操作を変更するには、Web サイトのカテゴリに対する操作を選択する (p. 181)を参照してください。

- **アダルト/ポルノ (ブロック)**: このカテゴリには、性具、CD-ROM およびビデオなどのアダルド製品のサイト、児童ポルノおよび小児性愛 (インターネット監視財団 (IWF) のブラックリストを含む) のサイト、ビデオチャット、エスコートサービス、ストリップクラブなどのアダルトサービスのサイト、エロチックな話や性行為の文章による描写のあるサイト、性描写のある漫画やアニメーションのサイト、性的に露骨なニュースグループやフォーラムなどのオンライングループのサイト、性的関連、エロチックなフルまたは部分的ヌードのあるサイト、性的に使用されている動物や無生物を含む、性行為の描写や画像のあるサイト、性的搾取または性的暴力を表す文章または画像のあるサイト、ボンデージ、フェティシズム、性器ピアスに関するサイト、ヌード画像

のあるナチュリストサイト、およびヌードを含むアダルト/フェティシズム写真のあるサイトが含まれます。

注
性の健康、乳ガン、または性感染症に関するサイトは対象外です (写実的な画像のあるサイトは対象になります)。

- **アルコール、タバコ (警告)**: このカテゴリには、アルコールやタバコ製品を無償または有償で促進/頒布するサイトが含まれます。
- **匿名プロキシ (ブロック)**: このカテゴリには、リモートプロキシや匿名ネットサーフィンに関するサイト、フィルタ処理を回避する検索エンジンのキャッシュ、およびフィルタリングを回避する Web ベースの翻訳サイトが含まれます。
- **犯罪行為 (ブロック)**: このカテゴリには、違法行為の実行を支持/指示/助言するサイト、法執行を回避するためのヒント、ピッキングおよび窃盗手法についてのサイトが含まれます。
- **ギャンブル (警告)**: このカテゴリには、現実の通貨や仮想通貨の使用を誘うオンラインギャンブルや宝くじサイト、賭け方や、宝くじ・ギャンブル・富くじへの参加に関する情報やアドバイスのあるサイト、仮想カジノやオフショアギャンブルのサイト、スポーツピックやくじのサイト、賞金が高額、または賭け金が高額の仮想スポーツリーグやシミュレーションリーグのサイトが含まれます。
- **ハッキング (ブロック)**: このカテゴリには、パスワードのハッキング、ウイルスの作成、または他のコンピュータやコンピュータ化された通信システムへのアクセス取得を目的として、機器やソフトウェアを疑わしい方法または不法に使用することの促進、指示、または助言を提供するサイト、フィルタリングソフトに関する指示や回避策を提供するサイト、クラッキングしたソフトおよび情報サイト、海賊版ソフトおよびマルチメディアのダウンロードサイト、およびコンピュータ犯罪サイトが含まれます。
- **違法薬物 (ブロック)**: このカテゴリには、工業利用以外の目的で違法薬物を製造/栽培するための方法/指示/キットを提供するサイト、アルコール、タバコ、違法薬物、およびその他未成年者に違法である薬物の使用を美化/奨励/指示したり、またはその使用を隠すことについてのサイト、シンナー遊び、処方薬の誤用、および他の合法薬物のの乱用を含む、「合法ドラッグ」に関する情報のあるサイト、違法薬物の無償または有償での頒布、麻薬道具の表示/販売およびその使用に関する記述のあるサイトが含まれます。
- **不寛容、差別問題 (ブロック)**: このカテゴリには、宗教、人種、国籍、性別、年齢、身体障害、または性的指向などに基づいて、特定の集団や団体に対する中傷や攻撃を奨励または扇動するサイト、人種、宗教、国籍、性別、年齢、身体障害、または性的指向に基づく、本質的に至上主義であり排他的な政治的/社会的な課題を奨励するサイト、ホロコースト修正主義/否認サイト、および憎悪を促進する他の修正主義サイト、ギャング[1] またはカルト[2]への入団を強制・勧誘するサイト、好戦性・過激派サイト、反対意見や信念を認識・尊重しないなど、甚だしく無神経/不快なコンテンツのあるサイトが含まれます。

注
上記の条件を含む、ニュース、歴史的事件、プレス記事などは対象外です (写実的な画像のあるサイトは対象になります)。

[1]ギャングとは、重罪の犯罪行為を主な活動内容とし、通称や独自のサインやマークを持ち、所属メンバが個人または集団でその団体の名の下に犯罪行為に関与する団体として定義されます。

[2] カルトは、団員の性格や行動を変えるような不当な影響を与えて、団員をごまかし、巧みに入団させ維持している団体として定義されます。 また、指導者が全権を握り、観念体系は全体主義で、個人の意思は団体に支配され、団体自体が、社会から団体を隔絶します。

- **フィッシング、詐欺 (ブロック)**: このカテゴリには、フィッシングや電話詐欺を行うサイト、電話サービス盗難の助言サイト、研究論文の販売サイトを含む、盗用・不正行為サイトが含まれます。
- **スパム URL (ブロック)**: このカテゴリには、特に、コンピュータ、金融・株、エンターテイメント、ゲーム、健康・医療、ユーモア・ノベルティ、出会い系、製品・サービス、ショッピング、トラベルなどに関するスパムに含まれる URL が含まれます。
- **スパイウェア (ブロック)**: このカテゴリには、悪質な実行可能ファイルやウイルス、サード パーティの監視や他の未承諾商用ソフトウェア、スパイウェアおよびマルウェアの「無断アクセス」の宛先など、エンドユーザーや組織に知られずに、またはエンドユーザーや組織の明示的な同意を得ずに、情報収集または追跡機能を提供または助長するサイトが含まれます。
- **悪趣味、不快 (警告)**: このカテゴリには、冗談、マンガ、風刺などを通じて、不快または暴力的な言葉を使用するサイト、冒涜的な言葉やわいせつなコンテンツの過剰使用のあるサイトが含まれます。
- **暴力 (警告)**: このカテゴリには、人間、動物、または団体に対する暴行を描写、記述、または奨励するサイト、拷問、切断、流血、恐ろしい死についての記述のあるサイト、摂食障害や依存症を含む、自殺または自傷の支持、奨励、描写のあるサイト、爆弾や他の有害または破壊的な装置を作成するための手順、材料、またはセットについての説明するサイト、テロ行為を奨励するサイト、ビデオゲームやオンラインゲームを含む、過剰に暴力的なスポーツやゲームのサイトが含まれます。

  注
  上記の条件を含む可能性がある、ニュース、歴史的事件、プレス記事などはブロックされません (写実的な画像のあるサイトは対象になります)。

- **武器 (警告)**: このカテゴリには、価格表や販売店の所在地を含む、オンラインでの購買または注文情報のあるサイト、銃、武器、弾薬、毒物の販売に関するコンテンツを主に含むか、そのようなコンテンツへのリンクを提供するページまたはサイト、銃、武器、弾薬、毒物の表示または使用法の詳しい説明のあるサイト、機関銃、自動火器、および他の攻撃用武器や狙撃手の訓練を提供するクラブのサイトが含まれます。

  注
  武器は、障害、打倒、または破壊に使用されるもの (こん棒、刃物、または銃など) として定義されます。

Web サイトのカテゴリに対する操作を選択する

Web コントロールを有効にし、「**不適切な Web サイトのコントロール**」ポリシーを選択すると、各 Web サイトのカテゴリに対するアクションを設定できます。また、デフォルトのポリシーに基づいた新規ポリシーを作成することもできます。詳細は、ポリシーを作成する (p. 31)を参照してください。

Web サイトのカテゴリに対する操作を選択する方法は次のとおりです。

1. 「**全般**」タブで、Web サイトのカテゴリの横にあるドロップダウンリストから、次のいずれか 1 つのアクションを選択してください。
   - **ブロック**: 選択したカテゴリに属する Web サイトへのユーザーアクアセスを阻止する。HTTP Web ページの場合、ブロック通知、およびその理由がユーザーに対して表示されます。HTTPS ページの場合は、バルーン ヒントがユーザーの Windows システムトレイに表示されます。

- **警告**: 社内の Web 使用ポリシーに違反する恐れがあることをユーザーに警告するが、続行を許可する。HTTP Web ページの場合、警告通知がユーザーに対して表示され、同サイトへのアクセスを続行することに対して注意を促します。HTTPS ページの場合は、通知がユーザーに対して表示されず、同サイトへのアクセスの続行が許可されます。このイベントは、「続行」イベントとして Enterprise Console に記録されます。
- **許可**: 選択したカテゴリに属する Web サイトへのユーザーアクアセスを許可する。このイベントはログに記録されません。

2. 「**OK**」をクリックします。

例外 Web サイトを管理する

「**不適切な Web サイトのコントロール**」ポリシーを選択済みの場合、「ブロック」および「警告」アクションの例外を作成できます。Web コントロールの対象から除外するには Web サイトを「許可する Web サイト」リストまたは「ブロックする Web サイト」リストに追加します。除外する項目は、IP アドレスやドメイン名で指定します。また、既存のエントリを編集したり、リストから Web サイトを削除したりすることもできます。

注
ブロックリストと許可リストの間で重複や整合性のとれない項目がある場合は、常にブロックリストの項目が優先されます。たとえば、ブロックリストと許可リストの両方に同じ IP アドレスが指定された場合、その Web サイトはブロックされます。さらに、ブロックリストにあるドメインのサブドメインが許可リストで指定された場合は、許可リストの設定は無視され、ドメインとそのサブドメインすべてがブロックされます。

例外 Web サイトを追加する方法は次のとおりです。

1. 「**例外 Web サイト**」タブで、「**許可する Web サイト**」または「**ブロックする Web サイト**」テキストボックスの横にある「**追加**」ボタンをクリックします。
2. 「**許可する Web サイトの追加**」ダイアログボックスで、「**ドメイン名**」、「**IP アドレスとサブネットマスク**」、または「**IP アドレス**」をクリックします。各形式の例は、該当するテキストボックスの上部に表示されます。
3. テキストボックスに、許可またはブロックする Web サイトのドメイン名や IP アドレスを入力します。
4. 「**OK**」をクリックします。

Web サイトを編集したり、リストから削除したりする場合は、該当する Web サイトを選択して、「**編集**」または「**削除**」をクリックします。

7.8.2 高度な Web コントロール

注
この機能はすべてのライセンスには含まれていません。利用するには追加購入が必要となります。詳細は、http://www.sophos.com/ja-jp/products/complete/comparison.aspxを参照してください。

Sophos Web Appliance、Sophos Management Appliance (どちらも国内未販売)、または Sophos UTM アプライアンス (バージョン 9.2 以降) を導入している場合は、Enterprise Console を使用して、ユーザーにアプライアンス ベースのポリシーを適用することができます。

エンドポイントコンピュータは、「不適切な Web サイトのコントロール」ポリシーを選択した場合と同様に Enterprise Console と通信しますが、Web コントロールのルールおよび Web のイベ

ントのログは、指定したアプライアンスと同期されます。ポリシーはエンドポイントコンピュータに保存され、最新のソフォスのデータに基づいて適用されます。

ユーザーアクセスは、Web コントロール ポリシーに基づいて、「ブロック」、「警告」、「許可」されます。ユーザーアクセスのデータは、Web Appliance または Management Appliance では「**レポート**」および「**検索**」機能から、UTM アプライアンスでは「**ログとレポート > Web プロテクション**」オプションから表示できます。Web コントロールのイベントはアプライアンスのログに記録されます。一方、Sophos Endpoint Security and Control のライブ URL フィルタリング (Web Protection) 機能でスキャン・評価されたサイトは、Enterprise Console に Web のイベントとして記録されます。

注
対応している全種類の Web ブラウザで、HTTP サイトと HTTPS サイトの両方がコントロールされますが、URL が HTTP か HTTPS によって Web Appliance や Management Appliance のユーザー通知の方法は異なります。HTTP サイトの場合、「ブロック」または「警告」に指定されたカテゴリに属するサイトにアクセスすると、ユーザーに通知ページが表示されます。HTTPS サイトの場合、サイトが「ブロック」されている場合のみユーザーに通知が表示され、通知は、バルーン ヒントとして Windows システムトレイに表示されます。「警告」に指定された HTTPS サイトにアクセスしても、ユーザー通知もログへの記録も行われません。代わりに、要求したページへのユーザーアクセスの続行が許可され、そのイベントは、Web Appliance または Management Appliance で「続行」されたアクションとしてログに記録されます。

UTM アプライアンスでは、エンドポイントコンピュータの監視と保護にクラウドベースの集中管理サービス、Sophos LiveConnect が使用されます。LiveConnect により、ローカルネットワーク上のエンドポイント、支社・支店、外出の多いユーザーのエンドポイントなど常にすべてのエンドポイントを管理できます。社内からネットワークに接続していない場合でも、ポリシーの更新内容がユーザーに配信され、エンドポイントコンピュータからレポートデータがアップロードされます。

Management Appliance または Web Appliance を使用している場合は、エンドポイントは直接または Sophos LiveConnect 経由でアプライアンスと通信を行えます。

「**高度な Web コントロール**」を選択すると、詳細機能に対応した Web コントロール ポリシーを使用することができます。高度な Web コントロール機能には、基本的な Web コントロール機能と比較して次のようなメリットがあります (使用しているアプライアンスにより異なります)。

- 50種類を超える URL のカテゴリに基づいて、ユーザーアクセスを警告またはブロックできる。
- 「特別の時間帯」用の専用のポリシーを適用できる。
- デフォルトまたは特定の時間帯用のポリシーにおける、ユーザーやグループごとの例外を指定する追加ポリシーを複数使用できる。
- 詳細なログやレポートを Web Appliance、Management Appliance または UTM アプライアンスで表示で きる。
- ユーザーがリモート接続する場合でも、LiveConnect を使用して、アップデート版ポリシーを適用したり、レポートデータをアップロードしたりできる。
- ブロックされた URL の処理に関するコメントをユーザーが送信できる。
- 企業ロゴを含むカスタマイズした通知ページや、固有のテキストをユーザーに対して表示できる。詳細は「Sophos Web Appliance」の製品ドキュメントを参照してください。
- SafeSearch が有効になっている場合、一般的な検索エンジン経由で、ユーザーが不適切な Web サイトにアクセスすることが自動的にブロックされる。

詳細な Web Appliance ポリシーの設定に関する情報は、Sophos Web Appliance の製品ドキュメントを参照してください。 http://wsa.sophos.com/docs/wsa/.

UTM アプライアンスの製品ドキュメントは、次のサイトから入手可能です。 http://www.sophos.com/ja-jp/support/documentation/sophos-utm.aspx

高度な Web コントロールを有効にする

注
以下の説明は、Sophos Web Appliance、Sophos Management Appliance、または Sophos UTM アプライアンス (バージョン 9.2 以降) がインストール・設定済みで、それが正常に動作しており、さらにエンドポイントにおける Web アクセス制御を使用していることを想定しています。

デフォルトで、Web コントロール ポリシーは無効になっています。次の手順を実行して、Web コントロールを有効にし、「高度な Web コントロール」ポリシーを使用してください。

注
ロールベースの管理を利用している場合は次の点に注意してください。

- Web コントロール ポリシーを編集するには、「**ポリシー設定 - Web コントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

高度な Web コントロールを有効にする方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どの Web コントロール ポリシーが適用されているか確認してください。詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**Web コントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
   「**Web コントロール ポリシー**」ダイアログボックスが表示されます。
3. 「**全般**」タブで、「**Web コントロールを有効にする**」をクリックします。
4. 「**高度な Web コントロール**」を選択します。
5. 「**設定**」パネルで、「**アプライアンスのホスト名** 」および「**Policy Exchange 用セキュリティキー**」を入力します。
   - Web Appliance または Management Applianceの場合、完全修飾ホスト名を入力する必要があります。セキュリティキーは、アプライアンスの「**Endpoint Web Control**」ページで表示されているキーと一致する必要があります。
   - UTM の場合は、UTM で使用されている Sophos LiveConnect のブローカーのホスト名と共有鍵を入力します。これらの情報は、UTM 管理インターフェースの WebAdmin で確認できます。「**Endpoint Protection** > **コンピュータ管理** > **詳細**」タブを開き、「**SEC 情報**」の下の「**Sophos LiveConnect – 登録**」というセクションを参照します。

   詳細は、Sophos Web Appliance の製品ドキュメント (http://wsa.sophos.com/docs/wsa/) を参照するか、または UTM アプライアンスの製品ドキュメント (http://www.sophos.com/ja-jp/support/documentation/sophos-utm.aspx) を参照してください。
6. 任意で「**Web サイトのカテゴリを識別できない場合は、閲覧をブロックする**」を選択することもできます。Web サイトのカテゴリに関するデータをエンドポイントコンピュータで取得できない場合、その機能が回復するまで、分類できない URLへのアクセスはブロックされます。
   デフォルトで、このチェックボックスは選択されていません。分類機能が動作していない場合でも、ユーザーは Web サイトにアクセスすることができます。
7. 「**OK**」をクリックします。

Enterprise Console は、Web Appliance、Management Appliance、または UTM で使用される Sophos LiveCennect ブローカーと通信できるよう、エンドポイントコンピュータを再設定します。

7.9 エクスプロイト対策ポリシー

注
この機能はすべてのライセンスには含まれていません。利用するには追加購入が必要となります。詳細は、http://www.sophos.com/ja-jp/products/complete/comparison.aspxを参照してください。

エクスプロイト対策の主な機能は次のとおりです。

- ランサムウェアから文書ファイルを保護する (CryptoGuard)。
- ブートセクタを攻撃から保護する (WipeGuard)。

重要
現在、サーバーでこの機能を使用することはできません。

- Web ブラウザの重要な機能を保護する (セーフブラウジング)。
- エクスプロイトを防止する。Java アプリケーションなど、最もマルウェアに悪用されやすいアプリケーションを保護します。
- プロセス書き換え攻撃から防御する。
- 信頼できないフォルダから .DLL ファイルが読み込まれることを阻止する。
- CPU のブランチトレースから保護する。

デフォルトでは、エクスプロイト対策機能とすべてのエクスプロイト対策のオプションは有効になっています。

重要
エクスプロイト対策機能が利用できるライセンスにアップグレードしても、既に管理下にあるコンピュータには、エクスプロイト対策機能は自動的にインストールされません。インストールするには、もう一度コンピュータを保護しなおす必要があります。詳細は、コンピュータを自動保護する (p. 45)を参照してください。

特定のアプリケーションをエクスプロイト対策の対象から除外するように設定できます。除外を設定した場合でも、CryptoGuard およびセーフブラウジングによる保護は解除されません。

エクスプロイト対策の推奨設定について、詳細は「Sophos Enterprise Console ポリシー設定ガイド」を参照してください。

注
ロールベースの管理を利用している場合は次の点に注意してください。

- エクスプロイト対策ポリシーを設定するには、「**ポリシー設定 - エクスプロイト対策**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

HitmanPro.Alert とポリシーのアップデート

HitmanPro.Alert は、エンドポイントに存在するセキュリティ保護が必要なアプリケーションを検出します。検出されたアプリケーションは、Sophos Enterprise Console のサーバーにレポートされます。サーバーでは、保護を要するアプリケーションの照合が行われ、2時間ごとに新しいアプリケーションのデータがポリシーに統合されます。更新されたポリシーは、サーバーからエンドポイントに配信され、保護を要するアプリケーションのリストが提供されます。

7.9.1 エクスプロイト対策を有効/無効に切り替える

ロールベースの管理を利用している場合は次の点に注意してください。

- エクスプロイト対策ポリシーを設定するには、「**ポリシー設定 - エクスプロイト対策**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

注
エクスプロイト対策機能とそのすべてのオプションは、デフォルトで有効になっています。

エクスプロイト対策を有効/無効に切り替える方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのエクスプロイト対策ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**エクスプロイト対策**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**エクスプロイト対策ポリシー**」ダイアログボックスの「**保護対策の設定**」タブで、「**エクスプロイト対策を有効にする**」チェックボックスを選択するか、または選択を外します。
4. 「**ランサムウェアから文書ファイルを保護する (CryptoGuard)**」チェックボックスを選択するか、または選択を外します。
   リモートで実行されるランサムウェアからの防御機能も有効/無効にできます (64ビットのエンドポイントのみ)。
5. 「**ディスクとブートレコードを保護する (WipeGuard)**」チェックボックスを選択するか、または選択を外します。
6. 「**Web ブラウザの重要な機能を保護する (セーフブラウジング)**」チェックボックスを選択するか、または選択を外します。

7. 「**脆弱なアプリケーションにおけるエクスプロイトを防止する**」チェックボックスを選択するか、または選択を外します。
   エクスプロイトから防御するアプリケーションの種類 (Microsoft Office アプリケーションなど) を選択することもできます。
8. 「**プロセス書き換え攻撃を防止する**」チェックボックスを選択するか、または選択を外します。
9. 「**信頼できないフォルダからの DLL の読み込みを防止する**」チェックボックスを選択するか、または選択を外します。
10. 「**CPU のブランチトレースを有効にする**」チェックボックスを選択するか、または選択を外します。
11. 「**OK**」をクリックします。

特定のアプリケーションをエクスプロイト対策の対象から除外するように設定できます。なお、除外を設定しても、CryptoGuard およびセーフブラウジングのオプションが選択されている場合、これらの保護は解除されません。詳細は、エクスプロイト対策の対象からアプリケーションを除外する (p. 187)を参照してください。

特定のエクスプロイトのイベントを、エクスプロイト対策の対象から除外することもできます。詳細は、エクスプロイト対策の対象からエクスプロイトのイベントを除外する (p. 188)を参照してください。

7.9.2 エクスプロイト対策の対象からアプリケーションを除外する

ロールベースの管理を利用している場合は次の点に注意してください。

- エクスプロイト対策ポリシーを設定するには、「**ポリシー設定 - エクスプロイト対策**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

重要
攻撃の対象になりやすいアプリケーションは、デフォルトで保護されます。エクスプロイト対策の対象からアプリケーションを除外する際は注意が必要です。除外を設定した場合でも、CryptoGuard およびセーフブラウジングによる保護は解除されません (エクスプロイト対策を有効/無効に切り替える (p. 186)を参照)。

特定のアプリケーションをエクスプロイト対策の対象から除外するように設定できます。以前に除外したアプリケーションを保護の対象に含めることもできます。

アプリケーションを除外する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのエクスプロイト対策ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**エクスプロイト対策**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**エクスプロイト対策ポリシー**」ダイアログボックスの「**アプリケーションの除外**」タブで、「**保護対象アプリケーション**」リストから除外するアプリケーションを選択し、「**除外**」をクリックします。
   選択したアプリケーションが「**除外するアプリケーション**」リストに移動します。

4. 除外したアプリケーションを保護の対象に含めるには、「**除外するアプリケーション**」リストから保護するアプリケーションを選択し、「**保護**」をクリックします。
5. 「**OK**」をクリックします。

7.9.3 エクスプロイト対策の対象からエクスプロイトのイベントを除外する

ロールベースの管理を利用している場合は次の点に注意してください。

- エクスプロイト対策ポリシーを設定するには、「**ポリシー設定 - エクスプロイト対策**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

重要

- エクスプロイトのイベントを除外する際、アプリケーション全体ではなく、特定のエクスプロイトのみが除外されます。
- 既に除外されているアプリケーションの一部であるエクスプロイトのイベントは、除外する必要はありません。

特定のエクスプロイトのイベントを、エクスプロイト対策の対象から除外できます。以前に除外したエクスプロイトのイベントを保護の対象に含めることもできます。

エクスプロイトのイベントを除外する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのエクスプロイト対策ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**エクスプロイト対策**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**エクスプロイト対策ポリシー**」ダイアログボックスの「**エクスプロイトの除外**」タブで、「**検出されたエクスプロイトのイベント**」リストから除外するエクスプロイトのイベントを選択し、「**除外**」をクリックします。
   選択したエクスプロイトのイベントが「**除外されたエクスプロイトのイベント**」リストに移動します。
4. 除外したエクスプロイトのイベントを保護の対象に含めるには、「**除外されたエクスプロイトのイベント**」リストから保護するイベントを選択し、「**保護**」をクリックします。
5. 「**OK**」をクリックします。

8 警告およびメッセージの設定

Enterprise Console には複数の種類の警告が表示されます。

- **コンソール画面に表示される警告**

  コンピュータで対処が必要なアイテムが発見されたり、エラーが生じた場合、Sophos Endpoint Security and Control から Enterprise Console に警告が送信されます。警告はコンピュータリストに表示されます。これらの警告の対処方法については、検出されたアイテムに関する警告に対処する (p. 51)を参照してください。

  この警告は、随時、表示されるので、設定の必要はありません。

- **コンソール画面に表示されるイベント**

  アプリケーション コントロール、ファイアウォール、パッチ評価、Web、データコントロール、デバイスコントロール、またはタンパー プロテクションに関連するイベント (ファイアウォールでアプリケーションがブロックされたなど) がエンドポイントコンピュータで発生すると、Enterprise Console に情報が送信されるため、該当するイベントビューアでイベントを参照できます。

- **指定した受信者に管理コンソールから送信される警告やメッセージ**

  コンピュータでアイテムが発見されると、デフォルトで、メッセージがコンピュータのデスクトップに表示され、Windows イベントログにエントリが追加されます。アプリケーション コントロール、データコントロール、またはデバイスコントロールのイベントが発生すると、当該のコンピュータのデスクトップにメッセージが表示されます。

  注
  ユーザーが任意に定義したデスクトップメッセージは、Windows 8 以降のコンピュータでは表示されません。

  さらに、管理者用のメール警告や SNMP メッセージを設定することもできます。

  注
  メール警告の送信にあたり、プロキシサーバーで認証を行う場合は、ソフォス サポートデータベースの文章 113780 を参照してください。

ここでは、指定した受信者に送信される警告の設定方法について説明します。

8.1 ソフトウェアのサブスクリプションの警告を設定する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**システム環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Enterprise Console では、アップデートマネージャが生成する警告が、「**アップデートマネージャ**」ビューの「**警告**」カラムに表示されます。ソフトウェアの固定バージョンにサブスクリプション登録している場合、同バージョンの製品サポートが終了間近である場合や終了した場合、警告が表示されます。製品ライセンスを変更した場合も警告が表示されます。

固定バージョンのソフトウェアにサブスクリプション登録している場合で、「**ソフォスのサポートが終了した固定バージョンのソフトウェアを自動アップグレードする**」オプションを選択している場合、サブスクリプションが自動的にアップグレードされます。

自動アップグレードオプションを選択していない場合、サブスクリプションを変更するよう警告が表示されます。

重要
製品サポートが終了しているソフトウェアを使用している場合、新しいセキュリティ脅威から保護されないことに注意してください。サポート中の製品への早急なアップグレードを推奨します。

また、サブスクリプション登録している製品バージョンのサポートが終了間近である場合や、サポートが終了した場合に、特定の宛先にメール警告を送信するよう設定できます。

1. 「**ツール**」メニューの「**メール警告の環境設定**」を選択します。
   「**メール警告の環境設定**」ダイアログボックスが表示されます。
2. SMTP 設定が設定されていない場合や、設定を表示したり変更したい場合は、「**環境設定**」をクリックします。
   「**SMTP の設定**」ダイアログボックスで、次のように詳細を設定します。
   a) 「**サーバーアドレス**」テキストボックスに、SMTP サーバーのホスト名や IP アドレスを入力します。
   b) 「**送信者**」テキストボックスに、バウンスメールや配信不能レポート (NDR) の送信先アドレスを入力します。
   c) 接続をテストする場合は、「**テスト**」をクリックします。
3. 「**受信者**」パネルで、「**追加**」をクリックします。
   「**メール警告受信者の追加**」ダイアログボックスが表示されます。
4. 「**メールアドレス**」フィールドに、受信者のアドレスを入力します。
5. 「**言語**」フィールドから、送信するメール警告の言語を選択します。
6. 「**サブスクリプション**」ペインで、指定した受信者に送信する「ソフトウェアのサブスクリプション」のメール警告を選択します。選択できる警告は次の 3種類です。
   - ソフトウェアのサブスクリプションに、サポート終了が間近なバージョンの製品が含まれている
   - ソフトウェアのサブスクリプションに、既に配信が終了しているバージョンの製品が含まれている
     この警告は、サブスクリプション登録している製品の製品サポートが終了した場合、または製品ライセンスを変更したため、新しいライセンスの下で特定の製品を使用できなくなった場合などに送信されます。
   - ソフォス製品のライセンス情報が更新されたため、製品の機能が変更されている可能性がある。

8.2 ウイルス対策および HIPS のメール警告を設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。

- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

グループ内のコンピュータで、ウイルス、疑わしい動作、不要と思われるアプリケーション、またはエラーが発見された場合、特定のユーザーにメールで警告を送信できます。

重要
Mac OS X コンピュータでは、複数のアドレスにメール警告を送信することはできません。

1. 「**ポリシー**」ペインで、変更するウイルス対策および HIPS ポリシーをダブルクリックします。
2. 「**ウイルス対策および HIPS ポリシー**」ダイアログボックスで、「**メッセージング**」をクリックします。
3. 「**メッセージング**」ダイアログボックスで、「**メール警告**」タブを開き、「**メール警告を送信する**」を選択します。
4. 「**送信するメールの内容**」パネルで、メール警告を送信するイベントの種類を選択します。

   注
   「**疑わしい動作の検知**」、「**疑わしいファイルの検出**」、「**アドウェアや不要と思われるアプリケーションの検出・クリーンアップ**」、および「**その他のエラー**」の設定内容は、Windows コンピュータにのみに適用されます。

5. 「**受信者**」パネルで、「**追加**」または「**削除**」ボタンをクリックして、メール警告の受信者アドレスを追加・削除します。追加したメールアドレスを変更するには、「**名前の変更**」をクリックします。

   重要
   Mac OS X コンピュータの場合、リスト最上部の受信者のみにメール警告が送信されます。

6. SMTP サーバーの設定内容や、メール警告で使用する言語を変更するには、「**SMTP の設定**」をクリックします。
7. 「**SMTP の設定**」ダイアログボックスで、次のように詳細を設定します。
   - 「**SMTP サーバー**」テキストボックスに、SMTP サーバーのホスト名、または IP アドレスを入力します。テスト用メール警告を送信する場合は、「**テスト**」をクリックします。
   - 「**SMTP 送信者アドレス**」テキストボックスに、バウンスメールや配信不能レポートの送信先アドレスを入力します。
   - 「**SMTP 返信先アドレス**」テキストボックスに、このメール警告に対する返信先アドレスを入力できます。メール警告は無人の送信専用メールボックスから送信されます。
   - 「**言語**」パネルで、ドロップダウン矢印をクリックして、メール警告で使用する言語を選択します。

8.3 ウイルス対策および HIPS の SNMP メッセージを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。

- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

グループ内のコンピュータでウイルスやエラーが発見された場合、特定のユーザーに SNMP メッセージを送信することができます。

注
ここでの設定内容は、Windows コンピュータのみに適用されます。

1. 「**ポリシー**」ペインで、変更するウイルス対策および HIPS ポリシーをダブルクリックします。
2. 「**ウイルス対策および HIPS ポリシー**」ダイアログボックスで、「**メッセージング**」をクリックします。
3. 「**メッセージング**」ダイアログボックスで、「**SNMP メッセージング**」タブを開き、「**SNMP メッセージを送信する**」を選択します。
4. 「**送信するメールの内容**」パネルで、Sophos Endpoint Security and Control から SNMP メッセージを送信するイベントの種類を選択します。
5. 「**SNMP トラップの宛先**」テキストボックスに、受信者の IP アドレスを入力します。
6. 「**SNMP コミュニティ名**」テキストボックスに、SNMP コミュニティ名を入力します。

8.4 ウイルス対策および HIPS のデスクトップメッセージを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトでは、ウイルス、疑わしいアイテム、または不要と思われるアプリケーションが検出されたコンピュータにデスクトップメッセージが表示されます。これらのメッセージは環境設定できます。

1. 「**ポリシー**」ペインで、変更するウイルス対策および HIPS ポリシーをダブルクリックします。
2. 「**ウイルス対策および HIPS ポリシー**」ダイアログボックスで、「**メッセージング**」をクリックします。
3. 「**メッセージング**」ダイアログボックスで、「**デスクトップメッセージ**」タブをクリックします。
   デフォルトで、「**デスクトップメッセージを送信する**」と、「**送信するメールの内容**」パネルのオプションすべてが選択されています。必要な場合は、これらの設定を編集します。

   注
   「**疑わしい動作の検知**」、「**疑わしいファイルの検出**」、および「**アドウェアや不要と思われるアプリケーションの検出**」の設定内容は Windows のみに適用されます。

4. 「**ユーザー定義メッセージ** 」テキストボックスには、標準のメッセージの終わりに追加するテキストを入力できます。

注
ユーザーが定義したデスクトップメッセージは、Windows 8 以降のコンピュータでは表示されません。

8.5 アプリケーション コントロールの警告やメッセージを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- アプリケーション コントロール ポリシーを設定するには、「**ポリシー設定 - アプリケーション コントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

管理対象アプリケーションが検出された際に、特定のユーザーに対してメッセージを送信することができます。

1. 「**ポリシー**」ペインで、変更するアプリケーション コントロールポリシーをダブルクリックします。
2. 「**アプリケーション コントロール ポリシー**」ダイアログボックスで、「**メッセージング**」タブを開きます。
   「**メッセージング**」パネルの「**デスクトップメッセージを送信する**」チェックボックスは、デフォルトで選択されています。未認証の管理対象アプリケーションがオンアクセス検索で検出・ブロックされた場合、デスクトップメッセージを表示し、アプリケーションがブロックされたことをユーザーに通知します。
3. 「**メッセージの内容**」ボックスに、標準のデスクトップメッセージの終わりに追加されるテキストを入力します。

   注
   ユーザーが定義したデスクトップメッセージは、Windows 8 以降のコンピュータでは表示されません。

4. 検出された管理対象アプリケーションに関するメール警告を送信する場合は、「**メール警告を送信する**」チェックボックスを選択します。
5. SNMP メッセージを送信する場合は、「**SNMP メッセージを送信する**」チェックボックスを選択します。

   注
   メール警告および SNMP メッセージングの設定内容および受信者は、ウイルス対策および HIPS ポリシーによって指定されます。詳細は、ウイルス対策および HIPS の SNMP メッセージを設定する (p. 191)を参照してください。

8.6 データコントロールの警告やメッセージを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- データコントロール ポリシーを設定するには、「**ポリシー設定 - データコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Enterprise Console で、機密情報の転送が検知またはブロックされると、イベントやメッセージが生成されます。

データコントロール ポリシーとイベントの詳細は、データコントロール ポリシー (p. 149)を参照してください。

データコントロールを有効にした場合に、記録されるイベントや、表示されるメッセージは次のとおりです。

- データコントロールのイベントログがクライアントマシンに記録されます。
- データコントロールのイベントが Enterprise Console に送信され、「**データコントロール - イベントビューア**」で表示できます。(イベントビューアを開くには、「**イベント**」メニューの「**データコントロールのイベント**」をクリックします。)

  注
  各エンドポイントコンピュータが Enterprise Console に送信できるデータコントロール イベントの件数は、1時間につき最大 50件です。

- 過去 1週間で、データコントロールのイベントが、しきい値を超えて発生したコンピュータの台数は、ダッシュボードに表示されます。
- デスクトップメッセージがクライアントマシンに表示されます。

また、次のメッセージを送信するよう、Enterprise Console を設定することもできます。

メール警告	指定した受信者にメール警告を送信します。
SNMP メッセージ	ウイルス対策および HIPS ポリシーの設定で指定した受信者に SNMP メッセージを送信します。

データコントロールのメッセージを設定する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのデータコントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**データコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
   「**データコントロール ポリシー**」ダイアログボックスが表示されます。
3. 「**データコントロール ポリシー**」ダイアログボックスで、「**メッセージング**」タブを開きます。デスクトップメッセージはデフォルトで有効になっています。また、「**一致したルールをメッセージに含める**」が選択されています。

4. ファイルが転送された際や、ファイルの転送をブロックした際に、確認メッセージを表示する場合は、標準のメッセージに付け加えるメッセージとして入力します。

   最大半角 100文字まで入力可能です。また、メッセージには、About Sophos といった HTML 形式のリンクを追加することもできます。

   注
   ユーザーが定義したデスクトップメッセージは、Windows 8 以降のコンピュータでは表示されません。

5. メール警告を有効にするには、「**メール警告を送信する**」チェックボックスを選択します。「**メール受信者**」フィールドに、受信者のメールアドレスを入力します。複数の受信者名はセミコロン「;」で区切ってください。
6. SNMP メッセージの送信を有効にするには、「**SNMP メッセージを送信する**」チェックボックスを選択します。

   メールサーバーと SNMP トラップの宛先は、ウイルス対策および HIPS ポリシーで設定します。

8.7 デバイスコントロールの警告やメッセージを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- デバイスコントロール ポリシーを編集するには、「**ポリシー設定 - デバイスコントロール**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Enterprise Console で、管理対象デバイスが検出またはブロックされると、イベントやメッセージが生成されます。

デバイス コントロール ポリシーとイベントの詳細は、デバイスコントロール ポリシー (p. 164)を参照してください。

デバイスコントロールを有効にした場合に、記録されるイベントや、表示されるメッセージは次のとおりです。

- デバイスコントロールのイベントログがクライアントマシンに記録されます。
- デバイスコントロールのイベントが Enterprise Console に送信され、「**デバイスコントロール - イベントビューア**」で表示できます。(イベントビューアを開くには、「**イベント**」メニューの「**デバイスコントロールのイベント**」をクリックします。)
- 過去 1週間で、デバイスコントロールのイベントが、しきい値を超えて発生したコンピュータの台数は、ダッシュボードに表示されます。
- デスクトップメッセージがクライアントマシンに表示されます。

また、次のメッセージを送信するよう、Enterprise Console を設定することもできます。

メール警告	指定した受信者にメール警告を送信します。
SNMP メッセージ	ウイルス対策および HIPS ポリシーの設定で指定した受信者に SNMP メッセージを送信します。

デバイスコントロールのメッセージを設定する方法は次のとおりです。

1. 設定するコンピュータのグループ (複数可) に、どのデバイスコントロール ポリシーが適用されているか確認してください。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 「**ポリシー**」ペインで、「**デバイスコントロール**」をダブルクリックします。次に、変更するポリシーをダブルクリックします。
3. 「**デバイスコントロール ポリシー**」ダイアログボックスの「**メッセージ**」タブで、デスクトップメッセージの表示がデフォルトで選択されています。メッセージの送信方法を詳細に設定するには、次の手順を実行してください。
   - デスクトップに表示するメッセージの内容を入力するには、「**メッセージの内容**」ボックスに、標準のメッセージの終わりに追加するテキストを入力します。
     最大半角 100文字まで入力可能です。また、メッセージには、About Sophos といった HTML 形式のリンクを追加することもできます。

     注
     ユーザーが定義したデスクトップメッセージは、Windows 8 以降のコンピュータでは表示されません。

   - メール警告を有効にするには、「**メール警告を送信する**」チェックボックスを選択します。「**メール受信者**」フィールドに、受信者のメールアドレスを入力します。複数の受信者名はセミコロン「;」で区切ってください。
   - SNMP メッセージの送信を有効にするには、「**SNMP メッセージを送信する**」チェックボックスを選択します。

   メールサーバーと SNMP トラップの宛先は、ウイルス対策および HIPS ポリシーで設定します。

8.8 ネットワークステータスのメール警告を設定する

ロールベースの管理を利用している場合、ネットワークステータスのメール警告を設定するには、「**システム環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

各ダッシュボード・パネルで警報・緊急レベルがしきい値を超えた場合、特定の宛先にメール警告を送信するように設定できます。

1. 「**ツール**」メニューの「**メール警告の環境設定**」を選択します。
   「**メール警告の環境設定**」ダイアログボックスが表示されます。
2. SMTP 設定が設定されていない場合や、設定を表示したり変更したい場合は、「**環境設定**」をクリックします。「**SMTP の設定**」ダイアログボックスで、次のように詳細を設定します。
   a) 「**サーバーアドレス**」テキストボックスに、SMTP サーバーのホスト名や IP アドレスを入力します。
   b) 「**送信者**」テキストボックスに、バウンスメールや配信不能レポート (NDR) の送信先アドレスを入力します。
   c) 接続をテストする場合は、「**テスト**」をクリックします。
3. 「**受信者**」パネルで、「**追加**」をクリックします。
   「**メール警告受信者の追加**」ダイアログボックスが表示されます。

4. 「**メールアドレス**」フィールドに、受信者のアドレスを入力します。
5. 「**言語**」フィールドから、送信するメール警告の言語を選択します。
6. 「**送信するメール警告の種類**」ペインで、指定した受信者に送信するメール警告を「警報レベルのしきい値の超過」と「緊急レベルのしきい値の超過」から選択します。

8.9 Active Directory との同期のメール警告を設定する

ロールベースの管理を利用している場合、Active Directory との同期のメール警告を設定するには、「**システム環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Active Directory との同期中にコンピュータやグループが新しく検出された際に、特定の宛先にメール警告を送信するように設定できます。同期したグループ内のコンピュータを自動保護する場合は、自動保護に失敗した場合に警告を送信するように設定することもできます。

1. 「**ツール**」メニューの「**メール警告の環境設定**」を選択します。
   「**メール警告の環境設定**」ダイアログボックスが表示されます。
2. SMTP 設定が設定されていない場合や、設定を表示したり変更したい場合は、「**環境設定**」をクリックします。
   「**SMTP の設定**」ダイアログボックスで、次のように詳細を設定します。
   a) 「**サーバーアドレス**」テキストボックスに、SMTP サーバーのホスト名や IP アドレスを入力します。
   b) 「**送信者**」テキストボックスに、バウンスメールや配信不能レポート (NDR) の送信先アドレスを入力します。
   c) 接続をテストする場合は、「**テスト**」をクリックします。
3. 「**受信者**」パネルで、「**追加**」をクリックします。
   「**メール警告受信者の追加**」ダイアログボックスが表示されます。
4. 「**メールアドレス**」フィールドに、受信者のアドレスを入力します。
5. 「**言語**」フィールドから、送信するメール警告の言語を選択します。
6. 「**送信するメール警告の種類**」ペインで、指定した受信者に送信するメール警告を「Active Directory の同期」から選択します。
   「Active Directory の同期」のメール警告の種類は次のとおりです。
   - 新規グループの検出
   - 新規コンピュータの検出
   - コンピュータの自動保護の失敗

8.10 Windows のイベントログを設定する

ロールベースの管理を利用している場合は次の点に注意してください。

- ここでのタスクを実行するには、「**ポリシー設定 - ウイルス対策および HIPS**」権限が必要です。
- 各ユーザーは、ユーザーごとのアクティブなサブ管理サイトに適用されているポリシーだけ編集できます。

詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

デフォルトで、Sophos Endpoint Security and Control は、ウイルス/スパイウェアを検出/クリーンアップしたとき、疑わしい動作/ファイルを検知したとき、またはアドウェア/不要と思われるアプリケーションを検出/クリーンアップしたときに、Windows のイベントログに警告を追加します。

これらの設定内容を編集する方法は次のとおりです。

1. 「**ポリシー**」ペインで、変更するウイルス対策および HIPS ポリシーをダブルクリックします。
2. 「**ウイルス対策および HIPS ポリシー**」ダイアログボックスで、「**メッセージング**」をクリックします。
3. 「**メッセージング**」ダイアログボックスで、「**イベントログ**」タブを開きます。
   デフォルトで、イベントログは有効になっています。必要に応じて設定内容を編集します。
   「**検索エラー**」には、Sophos Endpoint Security and Control で検索しようとしたアイテムへのアクセスが拒否された場合も含まれます。

8.11 ソフォスへのフィードバック送信を有効/無効に切り替える

ロールベースの管理を利用している場合、ソフォスへのフィードバック送信を有効/無効に切り替えるには、「**システム環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

Enterprise Console では、定期的にソフォスにレポートが送信されます。送信されるレポートは、製品の使用状況を反映した、製品やサービスの品質向上に役立てられます。収集される情報の種類や取り扱いに関する詳細は、以下よりソフォスのエンドユーザー使用許諾契約書 (EULA) や個人情報保護方針を参照してください。http://www.sophos.com/ja-jp/legal

EULA や個人情報保護方針に記載のとおり、送信される情報には任意のものと必須のものがあります。任意の情報については、「**ソフォスへのフィードバック送信**」設定を変更することで随時オプトアウト (情報の提供を停止) できます。

デフォルトで、ソフォスへのフィードバック送信は有効になっています。これは、Sophos Enterprise Console インストール ウィザードでコンソールをインストール、アップグレードする際、無効にすることができます。

インストール後、ソフォスへのフィードバック送信を有効/無効に切り替える場合は、次の操作を行ってください。

1. 「**ツール**」メニューで、「**ソフォスへのフィードバック送信**」をクリックします。
2. 「**ソフォスへのフィードバック送信**」ダイアログボックスで、ソフォスへのフィードバック送信を有効または無効に設定できます。
   - ソフォスへのフィードバック送信を有効に設定する場合は、利用規約をお読みになり、同意される場合は、「**同意する**」チェックボックスを選択してください。
   - ソフォスへのフィードバック送信を無効に設定する場合は、「**同意する**」チェックボックスの選択を外してください。

9 イベントの表示

アプリケーション コントロール、データコントロール、デバイスコントロール、ファイアウォール、パッチ評価、タンパー プロテクション、Web コントロール、またはエクスプロイト対策に関連するイベント (ファイアウォールでアプリケーションがブロックされたなど) がエンドポイントコンピュータで発生すると、Enterprise Console に情報が送信されるため、該当するイベントビューアでイベントを参照できます。

イベントビューアを利用して、ネットワークで発生したイベントを調査できます。また、任意に設定できるフィルタを使ってイベントの一覧を表示できます。たとえば、特定のユーザーが過去 1週間に発したデータコントールのイベントの一覧などを表示できます。

過去 1週間で、しきい値を超える数のイベントが発生したコンピュータの台数は、ダッシュボードに表示されます (タンパー プロテクションのイベントは、ダッシュボードには表示されません)。しきい値の設定方法については、ダッシュボードを環境設定する (p. 48)を参照してください。

また、イベントが発生した場合に特定の受信者に警告を送信するよう設定できます。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

9.1 アプリケーション コントロールのイベントを表示する

アプリケーション コントロールのイベントを表示する方法は次のとおりです。

1. 「**イベント**」メニューの「**アプリケーション コントロールのイベント**」をクリックします。
   「**アプリケーション コントロール - イベントビューア**」ダイアログボックスが表示されます。
2. 「**検索期間**」フィールドで、ドロップダウン矢印をクリックし、イベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
3. 特定のユーザーやコンピュータに関するイベントを表示するには、各フィールドに名称を入力します。
   フィールドを空欄のままにすると、すべてのユーザーおよびコンピュータに関するイベントが表示されます。
   各フィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
4. 特定のアプリケーションの種類に関するイベントを表示するには、「**アプリケーションのタイプ**」フィールドで、ドロップダウン矢印をクリックし、アプリケーションの種類を選択します。
   デフォルトで、イベントビューアには、すべての種類のアプリケーションに関するイベントが表示されます。
5. 「**検索**」をクリックし、イベントの一覧を表示します。

アプリケーション コントロールのイベントの一覧は、ファイルに出力できます。詳細は、イベントの一覧をファイルに出力する (p. 208)を参照してください。

9.2 データコントロールのイベントを表示する

注
ライセンスにデータコントロールが含まれない場合は、この機能は利用できません。

ロールベースの管理を利用している場合、Enterprise Console でデータコントロールのイベントを表示するには、「**データコントロールのイベント**」権限が必要です。ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

データコントロールのイベントを表示する方法は次のとおりです。

1. 「**イベント**」メニューの「**データコントロールのイベント**」をクリックします。
   「**データコントロール - イベントビューア**」ダイアログボックスが表示されます。
2. 「**検索期間**」フィールドで、ドロップダウン矢印をクリックし、イベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
3. 特定のユーザー、コンピュータ、またはファイルに関するイベントを表示するには、各フィールドに名称を入力します。
   フィールドを空欄のままにすると、すべてのユーザー、コンピュータ、およびファイルに関するイベントが表示されます。
   各フィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
4. 特定のルールに関するイベントを表示するには、「**ルール名**」フィールドで、ドロップダウン矢印をクリックし、ルール名を選択します。
   デフォルトで、イベントビューアには、すべてのルールに関するイベントが表示されます。
5. 特定のファイルの種類に関するイベントを表示するには、「**ファイルタイプ**」フィールドで、ドロップダウン矢印をクリックし、ファイルの種類を選択します。
   デフォルトで、イベントビューアには、すべての種類のファイルに関するイベントが表示されます。
6. 「**検索**」をクリックし、イベントの一覧を表示します。

データコントロールのイベントの一覧は、ファイルに出力できます。詳細は、イベントの一覧をファイルに出力する (p. 208)を参照してください。

9.3 デバイスコントロールのイベントを表示する

デバイスコントロールのイベントを表示する方法は次のとおりです。

1. 「**イベント**」メニューの「**デバイスコントロールのイベント**」をクリックします。
   「**デバイスコントロール - イベントビューア**」ダイアログボックスが表示されます。
2. 「**検索期間**」フィールドで、ドロップダウン矢印をクリックし、イベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
3. 特定のデバイスの種類に関するイベントを表示するには、「**デバイスタイプ**」フィールドで、ドロップダウン矢印をクリックし、デバイスの種類を選択します。
   デフォルトで、イベントビューアには、すべての種類のデバイスに関するイベントが表示されます。

注
「読み取り専用」に設定した光学ディスクドライブのイベントは、イベントビューアに表示されません。

4. 特定のユーザーやコンピュータに関するイベントを表示するには、各フィールドに名称を入力します。

   フィールドを空欄のままにすると、すべてのユーザーおよびコンピュータに関するイベントが表示されます。

   各フィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
5. 「**検索**」をクリックし、イベントの一覧を表示します。

「**デバイスコントロール - イベントビューア**」ダイアログボックスでは、デバイスコントロール ポリシーの対象からデバイスを除外できます。詳細は、デバイスをすべてのポリシーの対象から除外する (p. 169)を参照してください。

デバイスコントロールのイベントの一覧は、ファイルに出力できます。詳細は、イベントの一覧をファイルに出力する (p. 208)を参照してください。

9.4 ファイアウォールのイベントを表示する

エンドポイントで発生するファイアウォールのイベントは一度だけコンソールに送信されます。同じイベントが異なるエンドポイントで発生した場合は、「**ファイアウォール - イベントビューア**」にまとめて表示されます。異なるエンドポイントで発生したイベント数の合計は、「**カウント数**」カラムに表示されます。

ファイアウォールのイベントを表示する方法は次のとおりです。

1. 「**イベント**」メニューの「**ファイアウォールのイベント**」をクリックします。
   「**ファイアウォール - イベントビューア**」ダイアログボックスが表示されます。
2. 「**検索期間**」フィールドで、ドロップダウン矢印をクリックし、イベントを表示する対象期間を選択します。

   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
3. 特定の種類のイベントを表示するには、「**イベントタイプ**」フィールドで、ドロップダウン矢印をクリックし、イベントの種類を選択します。

   デフォルトで、イベントビューアには、すべての種類のイベントが表示されます。
4. 特定のファイルに関するイベントを表示するには、「**ファイル名**」フィールドにファイル名を入力します。

   フィールドを空欄のままにすると、すべてのファイルに関するイベントが表示されます。

   このフィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
5. 「**検索**」をクリックし、イベントの一覧を表示します。

「**ファイアウォール - イベントビューア**」ダイアログボックスでは、ファイアウォールのルールを作成できます。詳細は、ファイアウォールのイベントのルールを作成する (p. 119)を参照してください。

ファイアウォールのイベントの一覧は、ファイルに出力できます。詳細は、イベントの一覧をファイルに出力する (p. 208)を参照してください。

9.5 タンパー プロテクションのイベントを表示する

タンパー プロテクションのイベントには次の 2種類があります。

- タンパー プロテクションの認証に成功したときに記録されるイベント。認証済みのユーザーの名前と認証した日時が表示されます。
- ソフォス製品を改変しようとする操作が失敗したときに記録されるイベント。当該のソフォス製品またはコンポーネントの名前、発生日時、操作を行ったユーザーの名前が表示されます。

タンパー プロテクションのイベントを表示する方法は次のとおりです。

1. 「**イベント**」メニューの「**タンパー プロテクションのイベント**」をクリックします。
   「**タンパー プロテクション - イベントビューア**」ダイアログボックスが表示されます。
2. 「**検索期間**」フィールドで、ドロップダウン矢印をクリックし、イベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
3. 特定の種類のイベントを表示するには、「**イベントタイプ**」フィールドで、ドロップダウン矢印をクリックし、イベントの種類を選択します。
   デフォルトで、イベントビューアには、すべての種類のイベントが表示されます。
4. 特定のユーザーやコンピュータに関するイベントを表示するには、各フィールドに名称を入力します。
   フィールドを空欄のままにすると、すべてのユーザーおよびコンピュータに関するイベントが表示されます。
   各フィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
5. 「**検索**」をクリックし、イベントの一覧を表示します。

イベントの一覧は、ファイルに出力できます。詳細は、イベントの一覧をファイルに出力する (p. 208)を参照してください。

9.6 パッチ評価のイベント

注
ライセンスにパッチ評価が含まれない場合は、この機能は利用できません。

「**パッチ評価 - イベントビューア**」にはセキュリティパッチやパッチ評価の結果に関する情報がすべて表示されます。

「**パッチ情報**」フィールドには、パッチ情報のダウンロードのステータスが表示されます。次のいずれか 1つのステータスメッセージが表示されます。

- **ダウンロードされていません**: パッチ情報がダウンロードされていない、または、パッチ機能を使用できるライセンスがないことを意味します。
- **ダウンロード中です**: インストール後の初回のダウンロードが進行中であることを意味します。
- **最新です**: 最新のパッチ情報があることを意味します。
- **最新ではありません**: 過去 72時間以内にパッチデータのアップデートが正常に実行されていないことを意味します。通常このステータスは、ネットワーク接続の問題が原因で SEC が最新でない

場合に表示されます。また、パッチ機能を含む SEC のライセンスから含まないライセンスに変更した場合に表示されることもあります。このステータスメッセージは、アップデートが部分的に実行された場合にも表示されることがあります。

「**パッチ評価 - イベントビューア**」のタブは次のとおりです。

パッチの緊急度ごと

デフォルトで、このタブには、未適用のパッチが表示されます。各パッチに対して、そのパッチが適用されていないコンピュータの数、およびパッチに関連付けされている脅威と脆弱性が表示されます。なお、適用が必要なパッチの一覧、およびそれが未適用のコンピュータの数もフィルタリング表示できます。

未適用のパッチがあるコンピュータ

パッチ評価のステータスがコンピュータごとに表示されます。各コンピュータと未適用のパッチが表示されます。1台のコンピュータに複数の未適用パッチがある場合は、同じコンピュータが複数回表示されます。

9.6.1 パッチ評価のイベントを表示する

パッチ評価のイベントを表示する方法は次のとおりです。

1. 「**イベント**」メニューの「**パッチ評価のイベント**」をクリックします。
   「**パッチ評価 - イベントビューア**」ダイアログボックスが表示されます。
2. 「**パッチの緊急度ごと**」または「**未適用のパッチがあるコンピュータ**」のいずれかのタブをクリックします。各タブの詳細は、パッチ評価のイベント (p. 202)を参照してください。
3. 「検索条件」パネルで、特定のパッチに関するイベントを、パッチ名、コンピュータ名、脅威、または脆弱性ごとに表示するには、各欄に必要事項を入力します。利用可能な条件はタブに表示される情報と対応しています。

   フィールドを空欄のままにすると、すべてのパッチ名、パッチ ID、およびコンピュータ名に関するイベントが表示されます。

   各フィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
4. 特定のパッチに関するイベントを、ステータス、パッチの緊急度、ベンダ、グループ、またはリリース日ごとに表示するには、該当するフィールドのドロップダウン矢印をクリックして適切なオプションを選択します。利用可能な条件はタブに表示される情報と対応しています。

   デフォルトで、イベントビューアには、未適用のパッチの脅威レベル、ベンダ、グループ、脅威およびパッチ名が表示されます。
5. 「**検索**」をクリックし、パッチ評価のイベントの一覧を表示します。
   表示される結果については、検索結果のカテゴリ (p. 204)を参照してください。

各ハイパーリンクを右クリックすると、名前をコピーできます。また、「Ctrl+C」を押すと、パッチ評価のイベントの行をクリップボードにコピーできます。

パッチ評価のイベントの一覧は出力できます。詳細は、イベントの一覧をファイルに出力する (p. 208)を参照してください。

特定のパッチの詳細を表示するには、対応するリンクをクリックします。詳細は、パッチ、脅威、脆弱性の詳細を表示する (p. 204)を参照してください。

9.6.2 パッチ、脅威、脆弱性の詳細を表示する

パッチ、脅威、脆弱性の詳細を表示する方法は次のとおりです。

1. 「**イベント**」メニューの「**パッチ評価のイベント**」をクリックします。
   「**パッチ評価 - イベントビューア**」ダイアログボックスが表示されます。
2. 「**パッチの緊急度ごと**」または「**未適用のパッチがあるコンピュータ**」のいずれか 1つのタブをクリックし、必要なオプションを選択し、「**検索**」をクリックしてイベントの一覧を表示してください。
   表示される結果については、検索結果のカテゴリ (p. 204)を参照してください。
3. 詳細情報を表示するパッチ名をクリックします。
4. 「**パッチの詳細**」ダイアログボックスで、パッチの説明、修正される脆弱性や、その脆弱性を悪用する脅威に関する情報を表示できます。次の操作もできます (利用可能な場合)。
   - パッチ名をクリックし、Web ブラウザでベンダが提供するパッチ情報を参照する。
   - 脅威名をクリックし、Web ブラウザでソフォスの脅威解析情報やアドバイスを参照する。
   - 脆弱性名をクリックし、Web ブラウザで共通脆弱性識別子 CVE (Common Vulnerabilities and Exposures) を参照する。
   - 「**置き換え前のパッチ名**」カラムのパッチ名をクリックし、Web ブラウザからベンダーが提供するパッチの置き換え情報を参照する。

リストは、脅威名のアルファベット順、次に脆弱性のアルファベット順にソートされます。

9.6.3 検索結果のカテゴリ

検索結果は、各カテゴリに基づいて次のタブに表示されます。

- パッチの緊急度ごと (p. 204)
- 未適用のパッチがあるコンピュータ (p. 205)

パッチの緊急度ごと

検索結果は、次のカテゴリに基づいて表示されます。

- **脅威:**: 脅威とは、ウイルス、トロイの木馬、ワーム、スパイウェア、悪意のある Web サイトのほか、アドウェアやその他の業務上不要と思われるアプリケーションの総称です。脅威名をクリックし、Web ブラウザでソフォスの脅威解析情報やアドバイスを参照することができます。
- **脆弱性**: 脆弱性は、攻撃者に悪用される可能性のあるソフトウェアの弱点を指します。悪用されたことにより発生する被害は、脆弱性の種類や影響を受けたソフトウェアによって異なります。これ以上悪用されることがないよう、脆弱性を修正するためパッチは提供されます。脆弱性名をクリックし、Web ブラウザで共通脆弱性識別子 CVE (Common Vulnerabilities and Exposures) を参照できます。
- **パッチの緊急度**: パッチの緊急度は SophosLabs で指定されます。

  注
  未適用のパッチは、その緊急度に関わらず、すべて適用することを推奨します。

  — **緊急**: 修正される脆弱性のうち、1つ以上が悪用されることが、ほぼ確実なパッチです。

  — **高**: 修正される脆弱性のうち、1つ以上が高い確率で悪用されるパッチです。

  - **中**: 修正される脆弱性のうち、1つ以上が悪用される可能性のあるパッチです。
  - **低**: 修正される脆弱性が悪用される可能性の低いパッチです。
- **パッチ名**: パッチの名前を表示します。パッチ名をクリックすると、ベンダーが提供するパッチ情報を Web ブラウザに表示できます。
- **ベンダ**: パッチを公開したベンダの名前を表示します。
- **コンピュータ**: パッチが未適用のコンピュータの数を表示します。パッチが未適用のコンピュータがある場合は、その数をクリックして、「**未適用のパッチがあるコンピュータ**」タブで詳細を表示できます。ハイフン (-) が表示されている場合は、パッチ評価が行われていないことを示します。
- **置き換え後のパッチ名**: 置き換え後のパッチ名を表示します。パッチ名をクリックすると、「**パッチの詳細**」ダイアログボックスが表示され、置き換え後のパッチに関する情報が参照できます。
- **リリース日**: パッチのリリース日を表示します。

未適用のパッチがあるコンピュータ

検索結果は、次のカテゴリに基づいて表示されます。

- **コンピュータ**: パッチが未適用のコンピュータの名前を表示します。
- **パッチの緊急度**: パッチの緊急度は SophosLabs で指定されます。

  注
  未適用のパッチは、その緊急度に関わらず、すべて適用することを推奨します。

  - **緊急**: 修正される脆弱性のうち、1つ以上が悪用されることが、ほぼ確実なパッチです。
  - **高**: 修正される脆弱性のうち、1つ以上が高い確率で悪用されるパッチです。
  - **中**: 修正される脆弱性のうち、1つ以上が悪用される可能性のあるパッチです。
  - **低**: 修正される脆弱性が悪用される可能性の低いパッチです。
- **パッチ名**: パッチの名前を表示します。パッチ名をクリックすると、ベンダーが提供するパッチ情報を Web ブラウザに表示できます。
- **置き換え後のパッチ名**: 置き換え後のパッチ名を表示します。パッチ名をクリックすると、「**パッチの詳細**」ダイアログボックスが表示され、置き換え後のパッチに関する情報が参照できます。
- **前回の評価日時**: 未適用のパッチがあるか前回コンピュータを評価した日時を表示します。
- **ベンダ**: パッチを公開したベンダの名前を表示します。
- **リリース日**: パッチのリリース日を表示します。
- **グループ**: コンピュータが所属するグループの名前を表示します。

9.7 Web のイベントを表示する

注
ライセンスに Web コントロールが含まれない場合は、この機能は利用できません。

ロールベースの管理を利用している場合、Enterprise Console で Web のイベントを表示するには、「**Web のイベント**」権限が必要です。ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「Web - イベントビューア」で表示できる Web のイベントは次のとおりです。

- 「**ウイルス対策および HIPS** 」ポリシーの Web Protection 機能でブロックされた悪意のある Web サイト。
- Web コントロールのイベント (Web コントロール機能を使用した場合)。

Web のイベントの表示方法は、選択した Web コントロール ポリシーによって異なります。両方のポリシーモードで Web のイベントビューアを使用できますが、表示される内容は異なります。

「**不適切な Web サイトのコントロール**」ポリシーを選択した場合、「ブロック」および「警告」に指定されたサイトすべてにアクセスできます。なお、「警告」に指定されている HTTPS サイトにアクセスした場合、それは「続行」イベントとしてログに記録されます。Sophos Endpoint Security and Control において、HTTP サイトと HTTPS サイトの処理方法は異なります (不適切な Web サイトのコントロール (p. 178)を参照)。

「**高度な Web コントロール**」を選択した場合、イベントはアプライアンスに表示されます。

- Sophos Web Appliance や Management Appliance (共に日本では未販売) の場合、「**レポート**」および「**検索**」機能で閲覧履歴を表示できます。「ブロック」、「警告」、「許可」に関するイベントすべてが表示されます。なお、「警告」に指定されている HTTPS サイトにアクセスした場合、それは「続行」イベントとして表示されます。Sophos Endpoint Security and Control において、HTTP サイトと HTTPS サイトの処理方法は異なります (高度な Web コントロール (p. 182)を参照)。
- UTM の場合、「**ログとレポート** > **Web プロテクション** > **Webs使用状況レポート**」ページを使用します。このページには、Web サイトが (安全であるとして) クライアントに配信されたか、アプリケーションコントロールのルールによってブロックされたか、ユーザーがオーバーライド機能を使用してブロックされたページにアクセスしたかなどの動作が表示されます。

注
選択したポリシーに関わらず、Sophos Endpoint Security and Control のライブ URL フィルタリング (Web Protection (p. 101)) 機能でスキャン・評価された Web サイトは Enterprise Console に Web のイベントとして表示されます。

Web のイベントを表示する方法は次のとおりです。

1. 「**イベント**」メニューの「**Web のイベント**」をクリックします。
   「**Web - イベントビューア**」ダイアログボックスが表示されます。
2. 「**検索期間**」ボックスで、ドロップダウン矢印をクリックし、イベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
3. 特定の**ユーザー**や**コンピュータ**に関するイベントを表示するには、各フィールドに名称を入力します。
   フィールドを空欄のままにすると、すべてのユーザーおよびコンピュータに関するイベントが表示されます。
   各フィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
4. 特定のアクションに関連したイベントを表示するには、「**アクション**」フィールドで、ドロップダウン矢印をクリックし、アクションの種類を選択します。
5. 特定のドメインに関連したイベントを表示するには、ドメイン名を「**ドメイン**」フィールド入力します。
6. 特定の「**理由**」が原因で発生したイベントを表示するには、ドロップダウン矢印をクリックして、理由を選択します。
7. 「**検索**」をクリックし、イベントの一覧を表示します。

Web のイベントの一覧は、ファイルに出力できます。詳細は、イベントの一覧をファイルに出力する (p. 208)を参照してください。

9.7.1 最新の Web のイベントを表示する

最近ブロックした Web サイトなど、エンドポイントコンピュータで対処したイベントを新しいものから 10件表示できます。

最新の Web のイベントを表示する方法は次のとおりです。

1. 「**エンドポイント**」ビューのコンピュータのリストで、イベントを表示するコンピュータをダブルクリックします。
2. 「**コンピュータの詳細**」ダイアログボックスで、スクロールダウンして「**最新の Web のイベント**」セクションを表示します。

またレポートを作成して、イベントの数を各ユーザーごとに表示することもできます。詳細は、「ユーザーごとのイベント」レポートを設定する (p. 215)を参照してください。

9.8 エクスプロイト対策のイベントを表示する

注
ライセンスにエクスプロイト対策が含まれない場合、この機能は利用できません。

ロールベースの管理を利用している場合、Enterprise Console でエクスプロイト対策のイベントを表示するには、「**エクスプロイト対策のイベント**」権限が必要です。ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

エクスプロイト対策のイベントを表示する方法は次のとおりです。

1. 「**イベント**」メニューの「**エクスプロイト対策**」をクリックします。
   「**エクスプロイト対策 - イベントビューア**」ダイアログボックスが表示されます。
2. 「**検索期間**」ボックスで、ドロップダウン矢印をクリックし、イベントを表示する対象期間を選択します。
   「**過去 24時間**」など、固定期間を選択したり、「**カスタム**」を選択して、任意の開始・終了期間や時刻を指定することができます。
3. 特定の**ユーザー**や**コンピュータ**に関するイベントを表示するには、各フィールドに名称を入力します。
   フィールドを空欄のままにすると、すべてのユーザーおよびコンピュータに関するイベントが表示されます。
   各フィールドはワイルドカード文字に対応しています。任意の 1文字を指定する場合は、「?」を使用し、任意の文字列を指定する場合は、「*」を使用します。
4. 特定のタイプのイベントを表示するには、「**タイプ**」フィールドで、ドロップダウン矢印をクリックし、アクションの種類を選択します。
5. 「**検索**」をクリックし、イベントの一覧を表示します。

- エクスプロイト対策のイベントの一覧は、ファイルに出力できます。詳細は、イベントの一覧をファイルに出力する (p. 208)を参照してください。
- 特定のエクスプロイト対策のイベントを、エクスプロイト対策の対象から除外できます。詳細は、エクスプロイト対策の対象からイベントを除外する (p. 208)を参照してください。

9.9 イベントの一覧をファイルに出力する

アプリケーション コントロール、データコントロール、デバイスコントロール、ファイアウォール、パッチ評価、タンパー プロテクション、Web のイベント、またはエクスプロイト対策のイベントの一覧は、CSV 形式のファイル (カンマ区切り) に出力できます。また、パッチ評価のイベントの一覧を PDF ファイルに出力できます。

1. 出力するイベントの種類に応じて、「**イベント**」メニューから、適切な「イベント」オプションをクリックします。
   「**イベントビューア**」ダイアログボックスが表示されます。
2. 特定のイベントだけを表示する場合は、「**検索の条件**」ペインで、適宜フィルタを設定します。そして、「**検索**」をクリックしてイベントを表示します。
   詳細は、次のリンクを参照してください。
   - アプリケーション コントロールのイベントを表示する (p. 199)
   - データコントロールのイベントについて (p. 154)
   - デバイスコントロールのイベントについて (p. 165)
   - ファイアウォールのイベントを表示する (p. 201)
   - パッチ評価のイベント (p. 202)
   - タンパー プロテクションのイベントを表示する (p. 202)
   - Web のイベントを表示する (p. 205)
   - エクスプロイト対策のイベントを表示する (p. 207)
3. 「**エクスポート**」をクリックします。
4. 「**名前を付けて保存**」ウィンドウでファイルの出力先を参照して「**ファイル名**」ダイアログボックスにファイル名を入力し、「**ファイルの種類**」ダイアログボックスからファイルの種類を選択します。
5. 「**保存**」をクリックします。

9.10 エクスプロイト対策の対象からイベントを除外する

イベントビューアでアプリケーションやエクスプロイト対策のイベントを選択して、エクスプロイト対策の対象から除外できます。

1. 「**イベント**」メニューの「**エクスプロイト対策のイベント**」をクリックします。
   「**イベントビューア**」ダイアログボックスが表示されます。
2. 特定のイベントだけを表示する場合は、「**検索の条件**」ペインで、適宜フィルタを設定します。そして、「**検索**」をクリックしてイベントを表示します。
   詳細は、エクスプロイト対策のイベントを表示する (p. 207)を参照してください。
3. イベントをクリックして、「**除外**」をクリックします。
   「**エクスプロイト対策の除外**」ダイアログボックスが表示されます。
4. 変更するポリシーをクリックします。すべてのポリシーに対して設定を変更するには、「**すべて選択**」をクリックします。
5. 「**エクスプロイトイベント**」または「**アプリケーション**」パネルで、「**除外**」をクリックします。
6. 「**OK**」をクリックします。

選択したポリシーに対して、エクスプロイト対策のイベントやアプリケーションがエクスプロイト対策から除外されます。

10 レポートの作成

レポートは、ご使用のネットワークのセキュリティ・ステータスに関する多様な情報を、文字やグラフで提供します。

レポートは、「**レポートマネージャ**」で表示できます。「**レポートマネージャ**」では、既存のテンプレートを使用してレポートを迅速に作成したり、既存のレポートの設定を変更したり、一定の頻度でレポートを実行できます。また、作成したレポートを指定したメール受信者に添付ファイルとして送信することができます。また、レポートを印刷したり、複数の形式でエクスポートすることもできます。

ソフォスでは、そのまますぐ使えるレポートや、ニーズに合わせてカスタマイズできるレポートなどを用意しています。レポートの種類は次のとおりです。

- 警告とイベントの履歴
- 警告のサマリー
- 警告とイベント - アイテム名ごと
- 警告とイベント - 期間ごと
- 警告とイベント - 場所ごと
- ポリシー非準拠マシン
- ユーザーごとのイベント
- 管理対象エンドポイントの保護
- アップデート階層

レポートとロールベースの管理

ロールベースの管理を利用している場合、レポートを作成・編集・削除するには、「**レポート環境設定**」権限が必要です。この権限がない場合は、レポートの実行のみが可能です。ロールベースの管理の詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

レポートには、アクティブなサブ管理サイトからのデータのみを含めることができます。複数のサブ管理サイトを対象にしたレポートを作成することはできません。デフォルトのレポートは、**デフォルト**のサブ管理サイトから、作成した新しいサブ管理サイトにコピーされません。

サブ管理サイトを削除すると、当該のサブ管理サイトにあるレポートもすべて削除されます。

10.1 レポートを新規作成する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**レポート環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

レポートの作成方法は次のとおりです。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、「**作成**」をクリックします。
3. 「**レポートの新規作成**」ダイアログボックスで、レポートテンプレートを選択し、「**OK**」をクリックします。
   選択したテンプレートごとに表示される各ウィザードの指示に従ってレポートを作成します。

ウィザードを使用したくない場合は、「**レポートの新規作成**」ダイアログボックスで、「**ウィザードを使ってレポートを作成する**」チェックボックスを選択から外します。その後、レポートの「プロパティ」ダイアログボックスで、新規レポートを設定できます。詳細は、各レポートの設定に関する説明を参照してください。

10.2 「警告とイベントの履歴」レポートを設定する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**レポート環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「**警告とイベントの履歴**」レポートは、一定のレポート期間における警告とイベントを表示します。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、「**警告とイベントの履歴**」を選択し、「**プロパティ**」をクリックします。
3. 「**警告とイベントの履歴のプロパティ**」ダイアログボックスの「**環境設定**」タブで、オプションを指定します。

   a) 「**レポートの詳細**」パネルで、随時、レポートの名称と説明を編集します。

   b) 「**レポート期間**」パネルの「**期間**」テキストボックスで、ドロップダウン矢印をクリックして期間を選択します。

   「**先月**」など、固定期間を選択したり、「**カスタム**」を選択して、「**開始日**」・「**終了日**」ボックスに期間を指定することができます。

   c) 「**レポート場所**」パネルで、「**コンピュータのグループ**」または「**各コンピュータ**」をクリックします。そして、ドロップダウン矢印をクリックして、グループ名やコンピュータ名を指定します。

   d) 「**対象にする警告やイベントの種類**」パネルで、レポートに含める警告とイベントの種類を選択します。

   デフォルトで、全種類の警告とイベントがレポートの対象になります。

   または、特定の警告とイベントのみを表示することも可能です。特定の警告やイベント 1つを指定するには、「**詳細設定**」をクリックし、リストより警告名またはイベント名をクリックします。複数指定する場合は、テキストボックスで、ワイルドカード文字を使用して名前を入力します。名前の 1文字を指定する場合は、「?」を使用し、複数の文字を指定する場合は、「*」を使用します。例: 「W32/*」と入力すると、W32/ で始まるウイルス名すべてが指定されます。
4. 「**表示オプション**」タブで、警告とイベントの並び替え順序を選択します。

   デフォルトで、「**警告名とイベント名**」順に警告とイベントの詳細が表示されます。なお、「**コンピュータ名**」、コンピュータの「**グループ名**」、あるいは「**日時**」順に並び替えることもできます。
5. 一定の頻度でレポートを実行し、指定したメール受信者に添付ファイルとして送信するには、「**スケジュール**」タブで、「**このレポートをスケジュール設定する**」を選択します。開始日時とレポート作成の頻度を入力し、出力ファイルの形式および言語を指定し、レポート受信者のメールアドレスを入力します。

10.3 「警告のサマリー」レポートを設定する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**レポート環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「**警告のサマリー**」レポートには、ネットワークの総合的なセキュリティ ステータスの集計結果が表示されます。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、「**警告のサマリー**」を選択し、「**プロパティ**」をクリックします。
3. 「**警告のサマリーのプロパティ**」ダイアログボックスの「**環境設定**」タブで、オプションを指定します。

   a) 「**レポートの詳細**」パネルで、随時、レポートの名称と説明を編集します。

   b) 「**レポート期間**」パネルの「**期間**」テキストボックスで、ドロップダウン矢印をクリックして期間を選択します。

   「**先月**」など、固定期間を選択したり、「**カスタム**」を選択して、「**開始日**」・「**終了日**」ボックスに期間を指定することができます。
4. 「**表示オプション**」タブの「**結果の表示間隔**」で、1時間や 1日など、警告の頻度を算出する期間を指定する場合は、ドロップダウン矢印をクリックして期間を選択します。
5. 一定の頻度でレポートを実行し、指定したメール受信者に添付ファイルとして送信するには、「**スケジュール**」タブで、「**このレポートをスケジュール設定する**」を選択します。開始日時とレポート作成の頻度を入力し、出力ファイルの形式および言語を指定し、レポート受信者のメールアドレスを入力します。

10.4 「警告とイベント - アイテム名ごと」レポートを設定する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**レポート環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「**警告とイベント - アイテム名ごと**」レポートは、指定した期間における、すべてのコンピュータでのすべての警告とイベントに関する情報をアイテム名ごとにグループ分けして表示します。

レポートの設定方法は次のとおりです。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、「**警告とイベント - アイテム名ごと**」を選択し、「**プロパティ**」をクリックします。
3. 「**警告とイベント - アイテム名ごとのプロパティ**」ダイアログボックスの「**環境設定**」タブで、オプションを指定します。

   a) 「**レポートの詳細**」パネルで、随時、レポートの名称と説明を編集します。

   b) 「**レポート期間**」パネルの「**期間**」テキストボックスで、ドロップダウン矢印をクリックして期間を選択します。

   「**先月**」など、固定期間を選択したり、「**カスタム**」を選択して、「**開始日**」・「**終了日**」ボックスに期間を指定することができます。

   c) 「**レポート場所**」パネルで、「**コンピュータのグループ**」または「**各コンピュータ**」をクリックします。そして、ドロップダウン矢印をクリックして、グループ名やコンピュータ名を指定します。

   d) 「**対象にする警告やイベントの種類**」パネルで、レポートに含める警告とイベントの種類を選択します。

   デフォルトで、全種類の警告とイベントがレポートの対象になります。
4. 「**表示オプション**」タブの「**表示**」で、レポートで表示する警告とイベントを選択します。

   デフォルトで、すべての警告とイベント、および各発生件数が表示されます。

また、次の条件に一致した警告とイベントのみを表示するようにレポートを環境設定することもできます。

- 発生数の多い上位 n件の警告とイベント (n は任意の数値)、または
- m件以上の発生件数を上回った警告とイベント (m は任意の数値)

5. 「**並べ替え順序**」で、警告とイベントをアイテム数、または名前で並び替えるかを指定します。
   デフォルトで、発生件数の多い順に警告とイベントが表示されます。
6. 一定の頻度でレポートを実行し、指定したメール受信者に添付ファイルとして送信するには、「**スケジュール**」タブで、「**このレポートをスケジュール設定する**」を選択します。開始日時とレポート作成の頻度を入力し、出力ファイルの形式および言語を指定し、レポート受信者のメールアドレスを入力します。

10.5 「警告とイベント - 期間ごと」レポートを設定する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**レポート環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「**警告とイベント - 期間ごと**」レポートは、警告とイベントを一定の期間ごとにまとめて表示します。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、「**警告とイベント - 期間ごと**」を選択し、「**プロパティ**」をクリックします。
3. 「**警告とイベント - 期間ごとのプロパティ**」ダイアログボックスの「**環境設定**」タブで、オプションを指定します。

   a) 「**レポートの詳細**」パネルで、随時、レポートの名称と説明を編集します。

   b) 「**レポート期間**」パネルの「**期間**」テキストボックスで、ドロップダウン矢印をクリックして期間を選択します。
   「**先月**」など、固定期間を選択したり、「**カスタム**」を選択して、「**開始日**」・「**終了日**」ボックスに期間を指定することができます。

   c) 「**レポート場所**」パネルで、「**コンピュータのグループ**」または「**各コンピュータ**」をクリックします。そして、ドロップダウン矢印をクリックして、グループ名やコンピュータ名を指定します。

   d) 「**対象にする警告やイベントの種類**」パネルで、レポートに含める警告とイベントの種類を選択します。
   デフォルトで、全種類の警告とイベントがレポートの対象になります。
   または、特定の警告とイベントのみを表示することも可能です。特定の警告やイベント 1つを指定するには、「**詳細設定**」をクリックし、リストより警告名またはイベント名をクリックします。複数指定する場合は、テキストボックスで、ワイルドカード文字を使用して名前を入力します。名前の 1文字を指定する場合は、「?」を使用し、複数の文字を指定する場合は、「*」を使用します。例: 「W32/*」と入力すると、W32/ で始まるウイルス名すべてが指定されます。
4. 「**表示オプション**」タブで、毎時や毎日など、警告とイベントの頻度を算出する期間を指定する場合は、ドロップダウン矢印をクリックして期間を選択します。
5. 一定の頻度でレポートを実行し、指定したメール受信者に添付ファイルとして送信するには、「**スケジュール**」タブで、「**このレポートをスケジュール設定する**」を選択します。開始日時とレポート作成の頻度を入力し、出力ファイルの形式および言語を指定し、レポート受信者のメールアドレスを入力します。

10.6 「警告とイベント - 場所ごと」レポートを設定する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**レポート環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「**警告とイベント - 場所ごと**」レポートは、指定した期間における、すべてのコンピュータでのすべての警告に関する情報を場所ごとに分けて表示します。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、「**警告とイベント - 場所ごと**」を選択し、「**プロパティ**」をクリックします。
3. 「**警告とイベント - 場所ごとのプロパティ**」ダイアログボックスの「**環境設定**」タブで、オプションを指定します。

   a) 「**レポートの詳細**」パネルで、随時、レポートの名称と説明を編集します。

   b) 「**レポート期間**」パネルの「**期間**」テキストボックスで、ドロップダウン矢印をクリックして期間を選択します。

   「**先月**」など、固定期間を選択したり、「**カスタム**」を選択して、「**開始日**」・「**終了日**」ボックスに期間を指定することができます。

   c) 「**レポート場所**」パネルで、「**コンピュータ**」をクリックすると、コンピュータごとの警告数が表示され、「**グループ**」をクリックすると、コンピュータグループごとの警告が表示されます。

   d) 「**対象にする警告やイベントの種類**」パネルで、レポートに含める警告とイベントの種類を選択します。

   デフォルトで、全種類の警告とイベントがレポートの対象になります。

   または、特定の警告とイベントのみを表示することも可能です。特定の警告やイベント 1つを指定するには、「**詳細設定**」をクリックし、リストより警告名またはイベント名をクリックします。複数指定する場合は、テキストボックスで、ワイルドカード文字を使用して名前を入力します。名前の 1文字を指定する場合は、「?」を使用し、複数の文字を指定する場合は、「*」を使用します。例: 「W32/*」と入力すると、W32/ で始まるウイルス名すべてが指定されます。
4. 「**表示オプション**」タブの「**表示**」で、レポートで表示する場所を選択します。

   デフォルトで、すべてのコンピュータとグループ、および各発生件数が表示されます。次の情報のみを表示することもできます。

   - 警告とイベント数の多かった場所上位 n件 (n は任意の数値)、または
   - 警告とイベントが m件以上発生した場所 (m は任意の数値)
5. 「**並べ替え順序**」で、場所を検出アイテム数、または場所名で並び替えるかを指定します。

   デフォルトで、警告とイベント数の多い順 (アイテム数順) に場所が表示されます。場所をアルファベット順で表示する場合は、「**場所**」を選択してください。
6. 一定の頻度でレポートを実行し、指定したメール受信者に添付ファイルとして送信するには、「**スケジュール**」タブで、「**このレポートをスケジュール設定する**」を選択します。開始日時とレポート作成の頻度を入力し、出力ファイルの形式および言語を指定し、レポート受信者のメールアドレスを入力します。

10.7 「ポリシー非準拠マシン」レポートを設定する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**レポート環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「**ポリシー非準拠マシン**」レポートは、所属するグループのポリシーに準拠していないコンピュータの割合または台数を、一定の期間ごとにまとめて表示します。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、「**ポリシー非準拠マシン**」を選択し、「**プロパティ**」をクリックします。
3. 「**ポリシー非準拠マシンのプロパティ**」ダイアログボックスの「**環境設定**」タブで、オプションを指定します。
   a) 「**レポートの詳細**」パネルで、随時、レポートの名称と説明を編集します。
   b) 「**レポート期間**」パネルの「**期間**」テキストボックスで、ドロップダウン矢印をクリックして期間を選択します。
      「**先月**」など、固定期間を選択したり、「**カスタム**」を選択して、「**開始日**」・「**終了日**」ボックスに期間を指定することができます。
   c) 「**表示**」パネルで、レポートで表示するポリシーを選択します。デフォルトで、「**ウイルス対策および HIPS** 」ポリシーのみが選択されています。
4. 「**表示オプション**」タブの「**結果の表示間隔**」で、1時間や 1日など、警告の頻度を算出する期間を指定する場合は、ドロップダウン矢印をクリックして期間を選択します。
5. 「**結果の表示方法**」で、結果を割合または件数として表示することを指定します。
6. 一定の頻度でレポートを実行し、指定したメール受信者に添付ファイルとして送信するには、「**スケジュール**」タブで、「**このレポートをスケジュール設定する**」を選択します。開始日時とレポート作成の頻度を入力し、出力ファイルの形式および言語を指定し、レポート受信者のメールアドレスを入力します。

10.8 「ユーザーごとのイベント」レポートを設定する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**レポート環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「**ユーザーごとのイベント**」レポートは、アプリケーション コントロール、ファイアウォール、データコントロール、デバイスコントロール、および Web サイトに関するイベントをユーザーごとに分けて表示します。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、「**ユーザーごとのイベント**」を選択し、「**プロパティ**」をクリックします。
3. 「**ユーザーごとのイベントのプロパティ**」ダイアログボックスの「**環境設定**」タブで、オプションを指定します。
   a) 「**レポートの詳細**」パネルで、随時、レポートの名称と説明を編集します。
   b) 「**レポート期間**」パネルの「**期間**」テキストボックスで、ドロップダウン矢印をクリックして期間を選択します。

「**先月**」など、固定期間を選択したり、「**カスタム**」を選択して、「**開始日**」・「**終了日**」ボックスに期間を指定することができます。

c) 「**対象にするイベントの種類**」パネルで、イベントとして表示したいコンポーネントを選択します。

4. 「**表示オプション**」タブの「**表示**」で、レポートで表示するユーザーを選択します。

デフォルトで、すべてのユーザーと各イベント数が表示されます。次の情報のみを表示することもできます。

- イベント数の多かったユーザー上位 n件 (n は任意の数値)、または
- イベントが m件以上発生したユーザー (m は任意の数値)

5. 「**並べ替え順序**」で、ユーザーをイベント数、またはユーザー名で並び替えるかを指定します。

デフォルトで、イベント数の多い順にユーザーが表示されます。ユーザーをアルファベット順で表示する場合は、「**ユーザー**」を選択してください。

6. 一定の頻度でレポートを実行し、指定したメール受信者に添付ファイルとして送信するには、「**スケジュール**」タブで、「**このレポートをスケジュール設定する**」を選択します。開始日時とレポート作成の頻度を入力し、出力ファイルの形式および言語を指定し、レポート受信者のメールアドレスを入力します。

10.9 「管理対象エンドポイントの保護」レポートを設定する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**レポート環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

「**管理対象エンドポイントの保護**」レポートは、保護対象コンピュータの割合または台数を、一定の期間ごとにまとめて表示します。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、「**管理対象エンドポイントの保護**」を選択し、「**プロパティ**」をクリックします。
3. 「**管理対象エンドポイントの保護のプロパティ**」ダイアログボックスの「**環境設定**」タブで、オプションを指定します。

a) 「**レポートの詳細**」パネルで、随時、レポートの名称と説明を編集します。

b) 「**レポート期間**」パネルの「**期間**」テキストボックスで、ドロップダウン矢印をクリックして期間を選択します。

「**先月**」など、固定期間を選択したり、「**カスタム**」を選択して、「**開始日**」・「**終了日**」ボックスに期間を指定することができます。

c) 「**表示**」パネルで、レポートで表示するコンポーネントを選択します。

4. 「**表示オプション**」タブの「**結果の表示間隔**」で、1時間や 1日など、警告の頻度を算出する期間を指定する場合は、ドロップダウン矢印をクリックして期間を選択します。
5. 「**結果の表示方法**」で、結果を割合または件数として表示することを指定します。
6. 一定の頻度でレポートを実行し、指定したメール受信者に添付ファイルとして送信するには、「**スケジュール**」タブで、「**このレポートをスケジュール設定する**」を選択します。開始日時とレポート作成の頻度を入力し、出力ファイルの形式および言語を指定し、レポート受信者のメールアドレスを入力します。

10.10 アップデート階層レポート

「**アップデート階層**」レポートは、ネットワークにあるアップデートマネージャ、それによって管理されるアップデート共有フォルダ、および同共有フォルダをアップデート元とするコンピュータの数を表示します。

「**アップデート階層**」レポートを環境設定することはできません。レポートの実行方法は、レポートを実行する (p. 217)を参照してください。

10.11 レポートをスケジュール設定する

ロールベースの管理を利用している場合、ここでのタスクを実行するには、「**レポート環境設定**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

一定の頻度でレポートを実行し、指定したメール受信者に添付ファイルとして送信するよう設定することができます。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、スケジュール設定したいレポートを選択し、「**スケジュール**」をクリックします。
3. 表示されるダイアログボックスの「**スケジュール**」タブで、「**このレポートをスケジュール設定する**」を選択します。
4. レポート作成の開始日時、および頻度を入力します。
5. 出力ファイルの形式、および言語を指定します。
6. レポートの受信者のメールアドレスを入力します。

10.12 レポートを実行する

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、実行したいレポートを選択し、「**実行**」をクリックします。
   「**レポート**」ウィンドウに、レポートが表示されます。

レポートのレイアウトを変更したり、レポートを印刷したり、ファイルに出力することができます。

10.13 レポートを表またはグラフとして表示する

レポートの中には、表またはグラフのいずれかとして表示できるものがあります。この場合、レポートを表示する「**レポート**」ウィンドウに、「**表**」および「**グラフ**」という 2つのタブが表示されます。

1. ツールバーにある「**レポート**」アイコンをクリックします。
2. 「**レポートマネージャ**」ダイアログボックスで、「**警告とイベント - 場所ごと**」など、実行したいレポートを選択し、「**実行**」をクリックします。
   「**レポート**」ウィンドウに、レポートが表示されます。
3. レポートを表、またはグラフとして表示するには、該当するタブを選択してください。

10.14 レポートを印刷する

レポートを印刷する場合は、レポート上部のツールバーにある「**印刷**」アイコンをクリックします。

10.15 レポートをファイルへエクスポートする

レポートをファイルへエクスポートする方法は次のとおりです。

1. レポート上部のツールバーにある「**エクスポート**」アイコンをクリックします。

2. 「**レポートのエクスポート**」ダイアログボックスで、レポートをエクスポートするドキュメントやスプレッドシートの種類を選択します。
   選択できるオプションの種類は次のとおりです。
   - PDF - Acrobat
   - HTML
   - Microsoft Excel
   - Microsoft Word
   - リッチテキスト形式 - RTF
   - カンマ区切り - CSV
   - XML
3. 「**ファイル名**」の「参照」ボタンをクリックして、場所を選択します。そしてファイル名を入力します。「**OK**」をクリックします。

10.16 レポートのレイアウトを変更する

レポートのページレイアウトを変更することが可能です。たとえば、レポートを横方向 (幅の広いページ) に表示することができます。

1. レポート上部のツールバーにある「ページレイアウト」アイコンをクリックします。

2. 「**ページ設定**」ダイアログボックスで、用紙サイズ、印刷の向き、および余白を指定します。「**OK**」をクリックします。
   レポートは、ここで指定したページ設定を使用して表示されます。

これらの設定情報は、レポートを印刷したり、エクスポートする際にも使用されます。

11 監査

監査機能を使用すると、Enterprise Console の環境設定の変更、ユーザーやシステムによるアクションを監視することができます。この情報を、法令順守やトラブルシューティングに利用したり、また悪質な行為が発覚した際にはフォレンジック分析に利用したりすることができます。

デフォルトで監査は無効になっています。監査を有効にすると、特定の環境設定に変更が生じたり、特定のアクションが実行された場合に、監査データベースに監査エントリが書き込まれます。

注
ロールベースの管理を利用している場合、監査を有効化または無効化するには、「**監査**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

監査エントリには以下の情報が含まれます。

- 実行されたアクション
- アクションを実行したユーザー
- ユーザーのコンピュータ名
- ユーザーのサブ管理サイト
- アクションの実行日時

成功および失敗したアクションの両方が監査され、監査エントリには、システムでアクションを実行したユーザー名、および正しく終了しなかったアクションを開始したユーザー名が表示されます。

監査対象のアクションは次のとおりです。

カテゴリ	アクション
コンピュータによるアクション	警告およびエラーの消去/解決、コンピュータの保護、コンピュータのアップデート、コンピュータの削除、コンピュータでのシステムのフル検索の実行
コンピュータグループの管理	グループの作成、グループの削除、グループの移動、グループ名の変更、グループへのコンピュータの割り当て
ポリシーの管理	ポリシーの作成、ポリシー名の変更、ポリシーの複製、ポリシーの編集、コンピュータへのポリシーの割り当て、ポリシーの製品出荷時へのリセット、ポリシーの削除
ロールの管理	ロールの作成、ロールの削除、ロール名の変更、ロールの複製、ロールへのユーザーの追加、ロールからのユーザーの削除、ロールからの権限の削除
アップデートマネージャの管理	アップデートマネージャのアップデート、アップデートマネージへの環境設定の適用、警告の消去、アップデートマネージャの消去、アップデートマネージャの環境設定、新しいソフトウェアのサブスクリプションの追加、ソフトウェアのサブスクリプションの削除、ソフトウェアのサブスクリプション名の変更、ソフトウェアのサブスクリプションの編集、ソフトウェアのサブスクリプションの複製

カテゴリ	アクション
システムイベント	監査の有効化、監査の無効化

監査データベースに保存されているデータは、Microsoft Excel、Microsoft Access、Microsoft SQL Server Reporting Services や Crystal Reports などの他社製プログラムを使用してアクセスし、解析できます。監査エントリの表示方法についての詳細は、「Sophos Enterprise Console監査ユーザーガイド」を参照してください。

11.1 監査を有効/無効に切り替える

ロールベースの管理を利用している場合、監査を有効化または無効化するには、「**監査**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

監査を有効/無効に切り替える方法は次のとおりです。

1. 「**ツール**」メニューで「**監査の管理**」をクリックします。
2. 「**監査の管理**」ダイアログボックスで、「**監査を有効にする**」チェックボックスを選択または選択解除して、監査を有効/無効に切り替えます。このオプションはデフォルトで無効になっています。

12 Enterprise Console でのデータのコピー、印刷

12.1 コンピュータのリストのデータをコピーする

「**エンドポイント**」ビューのコンピュータのリストに表示されるデータは、クリップボードにコピーし、タブ区切り形式で他のドキュメントに貼り付けることができます。

1. 「**エンドポイント**」ビューの「**グループ**」ペインで、データをコピーするコンピュータのグループを選択します。
2. 「**表示**」ドロップダウンリストから、「**問題があると思われるコンピュータ**」など、表示するコンピュータを選択します。
3. 対象のグループにサブグループがある場合は、検索対象を「**このレベルのみ**」または「**このレベル以下**」のどちらかに指定します。
4. コンピュータのリストで、「**ウイルス対策の詳細**」など、表示するタブを選択します。
5. コンピュータのリストをクリック (リスト内ならどこでもよい) します。これでリストが選択されたことになります。
6. 「**編集**」メニューの「**コピー**」をクリックし、クリップボードにデータをコピーします。

12.2 コンピュータのリストのデータを印刷する

「**エンドポイント**」ビューのコンピュータのリストに表示される情報を印刷できます。

1. 「**エンドポイント**」ビューの「**グループ**」ペインで、データを印刷するコンピュータのグループを選択します。
2. 「**表示**」ドロップダウンリストから、「**問題があると思われるコンピュータ**」など、表示するコンピュータを選択します。
3. 対象のグループにサブグループがある場合は、検索対象を「**このレベルのみ**」または「**このレベル以下**」のどちらかに指定します。
4. コンピュータのリストで、「**ウイルス対策の詳細**」など、表示するタブを選択します。
5. コンピュータのリストをクリック (リスト内ならどこでもよい) します。これでリストが選択されたことになります。
6. 「**ファイル**」メニューの「**印刷**」をクリックします。

12.3 コンピュータの詳細をコピーする

「**コンピュータの詳細**」ダイアログボックスに表示される情報は、クリップボードにコピーし、他のドキュメントに貼り付けることができます。この情報には、コンピュータ名、OS、インストールされているセキュリティソフトのバージョン、未対処の警告とエラー、更新状況などが含まれます。

1. 「**エンドポイント**」ビューのコンピュータのリストで、データをコピーするコンピュータをダブルクリックします。
2. 「**コンピュータの詳細**」ダイアログボックスで、「**コピー**」をクリックし、クリップボードにデータをコピーします。

12.4 コンピュータの詳細を印刷する

「**コンピュータの詳細**」ダイアログボックスから、コンピュータに関する情報を印刷することができます。この情報には、コンピュータ名、OS、インストールされているセキュリティソフトのバージョン、未対処の警告とエラー、更新状況などが含まれます。

1. 「**エンドポイント**」ビューのコンピュータのリストで、データを印刷するコンピュータをダブルクリックします。
2. 「**コンピュータの詳細**」ダイアログボックスで、「**印刷**」をクリックします。

13 トラブルシューティング

「コンピュータの保護」ウィザードを実行した際に、セキュリティソフトのインストールに失敗することがありますが、考えられる原因は次のとおりです。

- 使用している OS で自動インストールを実行することができない。この場合は、手動でインストールを行います。他の OS の保護がライセンスで許諾されている場合は、その詳細について「スタートアップガイド Linux/UNIX 版」を参照してください。
- OS が認識されない。これは、コンピュータの検索を行った際に、「ドメイン¥ユーザー名」形式でユーザ名を入力しなかったことが原因の場合があります。
- セキュリティ対策ソフトを展開するために必要なアクセスが、ファイアウォールのルールによってブロックされている。

13.1 コンピュータでオンアクセス検索が稼動していない

オンアクセス検索が稼動していないコンピュータがある場合は、次の点を確認してください。

1. 各コンピュータに、どのウイルス対策および HIPS ポリシーが指定されているか確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 同ポリシー内でオンアクセス検索が有効になっており、コンピュータがそのポリシーに準拠していることを確認します。
   詳細は、オンアクセス検索を有効/無効に切り替える (p. 84)、およびコンピュータにグループ固有のポリシーを適用する (p. 33)を参照してください。

13.2 ファイアウォールが無効になっている

ファイアウォールが無効になっているコンピュータがある場合は、次の点を確認してください。

1. 各コンピュータで使用しているファイアウォールポリシーを確認します。
   詳細は、グループに適用されているポリシーを確認する (p. 26)を参照してください。
2. 同ポリシー内でファイアウォールが有効になっており、コンピュータがそのポリシーに準拠していることを確認します。
   詳細は、ファイアウォールを一時的に無効にする (p. 120)、およびコンピュータにグループ固有のポリシーを適用する (p. 33)を参照してください。

13.3 ファイアウォールがインストールされていない

注
ロールベースの管理を利用している場合、ファイアウォールをインストールするには「**コンピュータの検索、保護、およびグループ**」権限が必要です。詳細は、ロールとサブ管理サイトを管理する (p. 14)を参照してください。

エンドポイントコンピュータにクライアントファイアウォールをインストールする前に、各コンピュータで Windows クライアント OS を稼働していることを確認してください。

注
サーバー OS や Windows Vista Starter を稼動しているコンピュータに、Sophos Client Firewall をインストールすることはできません。

ファイアウォールをインストールするコンピュータがある場合は、次の操作を行ってください。

1. コンピュータを選択し、右クリックして、「**コンピュータの保護**」を選択します。
   「**コンピュータの保護 ウィザード**」が表示されます。「**次へ**」をクリックします。
2. 機能を選択するようメッセージが表示されるので、「**Firewall**」を選択します。ウィザードを完了します。

引き続きこの問題が発生する場合は、ソフォス テクニカルサポートへお問い合わせください。

13.4 コンピュータに未対処の警告がある

- ウイルスや、使用を許可したくないアプリケーションのあるコンピュータがある場合は、コンピュータを直ちにクリーンアップする (p. 54)を参照してください。
- **使用したい**アドウェア/不要と思われるアプリケーションのあるコンピュータがある場合は、アドウェアや不要と思われるアプリケーションを認証する (p. 109)を参照してください。
- 最新版のないコンピュータがある場合は、最新版のないコンピュータをアップデートする (p. 78)を参照して、問題の解析・解決に役立ててください。

注
警告の表示は、必要なくなった時点で消去することができます。警告のあるコンピュータを選択し、右クリックして、「**警告とエラーの対処**」を選択してください。警告またはエラーを消去するには、「**修復 - クリーンアップ**」権限が必要です。

13.5 コンピュータがコンソールの管理下にない

Windows、Mac、Linux、および UNIX コンピュータのアップデート・監視を行うためには、Enterprise Console を使って管理する必要があります。

注
Active Directory との同期 (ロールとサブ管理サイトを管理する (p. 14)を参照) を行っていない場合、コンソールはネットワークに新しく追加されたコンピュータを自動的に表示・管理しません。ツールバーで「**コンピュータの検出**」をクリックして、追加したコンピュータを検索し、「**グループ外のコンピュータ**」フォルダに配置してください。

管理対象外のコンピュータの詳細は、「**ステータス**」タブでグレーアウト表示されています。

管理対象外のコンピュータを管理下におくには、次の操作を行ってください。

1. 「**表示**」ドロップダウンリストで、「**管理対象外のコンピュータ**」を選択します。
2. 次のいずれかの手順を実行してください。
   - 管理対象外のコンピュータが、「**グループ外のコンピュータ**」フォルダにある場合、そのコンピュータを選択し、配置先のグループにドラッグ & ドロップして配置します。「**コンピュータの保護 ウィザード**」が起動されるので、指示に従ってコンピュータを保護してください。
   - コンピュータがすでにグループに属している場合は、そのコンピュータを選択して右クリックし、「**コンピュータの保護**」を選択して、管理対象バージョンの Sophos Endpoint Security and Control をインストールします。
3. Enterprise Console が Sophos Endpoint Security and Control を自動的にインストールできないコンピュータがある場合は、手動インストールを行ってください。

   「**コンピュータの保護 ウィザード**」を使用した自動インストールは、Windows コンピュータのみで実行できます。Mac、Linux または UNIX のコンピュータを保護する場合は、手動でソフトウェアをインストールしてください。

   Mac や Windows コンピュータを手動で保護する方法については、「Sophos Enterprise Console アドバンス スタートアップガイド」を参照してください。

   Linux または UNIX コンピュータを保護する方法については、「Sophos Enterprise Console スタートアップガイド Linux/UNIX 版」を参照してください。

13.6 「グループ外のコンピュータ」フォルダにあるコンピュータを保護することができない

「**グループ外のコンピュータ**」フォルダには、ユーザーが作成したグループに配置されていないコンピュータだけが入っています。これらのコンピュータにポリシーを適用することはできません。グループに配置するまで、コンピュータを保護することはできません。

13.7 Sophos Endpoint Security and Control のインストールに失敗する

「**コンピュータの保護ウィザード**」で、コンピュータに Sophos Endpoint Security and Control をインストールできない場合は、次のような原因が考えられます。

- 各コンピュータでどの OS を稼動しているか Enterprise Console が把握していない。これは、コンピュータの検索を行う際、ドメイン名¥ユーザー名 という形式でユーザー名を入力しなかったためと考えられます。
- 使用している OS で自動インストールを実行することができない。この場合は、手動でインストールを行います。操作方法は、「Sophos Enterprise Console アドバンス スタートアップガイド」を参照してください。

- コンピュータで他のファイアウォールが起動している。
- Windows XP コンピュータ上の「簡易ファイルの共有」が無効になっていない。
- Windows Vista コンピュータで、「共有ウィザードを使用する」オプションが無効になっていない。
- コンピュータの OS でサポートされていない機能をインストールしようとした。

Sophos Endpoint Security and Control の機能のシステム要件の一覧は、ソフォス Web サイトのシステム要件ページ (http://www.sophos.com/ja-jp/products/all-system-requirements) を参照してください。

13.8 コンピュータがアップデートされない

最新版のないコンピュータをアップデートする (p. 78)を参照して、問題の解析・解決に役立ててください。

13.9 ウイルス対策の設定が Mac に適用されない

ウイルス対策設定の中には、Mac に適用されないものもあります。この場合は、設定を行うページに警告が記載されます。

Mac 環境に適用するウイルス対策および HIPS ポリシーの設定についての詳細は、ソフォスのサポートデータベースの文章 118859 を参照してください。

13.10 ウイルス対策の設定が Linux または UNIX コンピュータに適用されない

ウイルス対策設定の中には、Linux または UNIX コンピュータに適用されないものもあります。この場合は、設定を行うページに警告が記載されます。

Linux コンピュータでは、「Sophos Anti-Virus for Linux 環境設定ガイド」に説明のある savconfig コマンドおよび savscan コマンドを使用して設定を変更することができます。

UNIX コンピュータでは、「Sophos Anti-Virus for UNIX 環境設定ガイド」に説明のある savscan コマンドを使用して設定を変更することができます。

13.11 Linux または UNIX コンピュータにポリシーが指定されていない

CID でコーポレート環境設定ファイルを使用し、そのファイルにポリシーと競合する環境設定の値が含まれている場合、そのコンピュータは、「ポリシーと異なる」として表示されます。

「**ポリシーの適用**」オプションを指定しても、CID ベースの環境設定がコンピュータに再適用されるまでの間、一時的にポリシーが適用されるに過ぎません。

この問題を解決するには、コーポレート環境設定ファイルを再検討し、可能な限り、コンソールベースの環境設定で置き換えてください。

13.12 予期しない新規検索が Windows コンピュータに表示される

Windows コンピュータにある Sophos Endpoint Security and Control の「検索」の一覧を参照すると、ユーザーが作成していないにもかかわらず、新しく「実行可能な検索」が表示されている場合があります。

この新規検索は、コンソール画面で設定したスケジュール検索です。削除しないようにしてください。

13.13 接続速度が遅い、またはタイムアウトになる

Enterprise Console とネットワークコンピュータ間の通信速度が遅くなったり、コンピュータが反応しなくなる場合は、接続速度に問題があることが考えられます。

ソフォス ネットワーク通信レポートを表示して、コンピュータと Enterprise Console 間の現在の通信状況の概要を参照してください。このレポートを表示するには、問題の発生したコンピュータで次の操作を行います。タスクバーで、「**スタート**」ボタンをクリックし、「**すべてのプログラム > Sophos > Sophos Endpoint Security and Control**」を選択します。次に、「**ソフォス ネットワーク通信レポートの表示**」をクリックします。

レポートは、問題の可能性がある領域を表示し、問題が検知された場合は、その対処方法を表示します。

13.14 アドウェアや不要と思われるアプリケーションが検出されない

アドウェアや他の不要と思われるアプリケーションが検出されない場合、次の点を確認してください。

- 検出が有効に設定されている。詳細は、オンアクセス検索を環境設定する (p. 82)を参照してください。
- アプリケーションが Windows コンピュータにある。

13.15 アイテムが部分的に検出される

Sophos Endpoint Security and Control は、アイテム (例: トロイの木馬や不要と思われるアプリケーション) の「部分的な検出」をレポートすることがあります。これは、アプリケーションに含まれるすべてのコンポーネントが検出されなかったことを意味します。

検出されなかった他のコンポーネントを検索するには、対象のコンピュータでシステムのフル検索を実行する必要があります。Windows コンピュータでは、対象のコンピュータを選択し、右クリックして、「**システムのフル検索**」を選択してください。また、アドウェアや他の不要と思われるアプリケーションに対するスケジュール検索を設定することもできます。詳細は、オンアクセス検索を環境設定する (p. 82)およびスケジュール検索を作成する (p. 89)を参照してください。

この操作を行っても、依然としてアプリケーションの全コンポーネントが検出されない場合は、次の原因が考えられます。

- 十分なアクセス権限がない
- アプリケーションのコンポーネントが含まれるコンピュータ上の一部のドライブまたはフォルダが検索から除外されている

2つ目の理由が原因と思われる場合、検索から除外する項目のリストを確認してください (オンアクセス検索の対象から項目を除外する (p. 87)を参照)。リストに項目がある場合はリストから削除し、再度コンピュータの検索を実行してください。

Sophos Endpoint Security and Control は、アドウェアや他の不要と思われるアプリケーションのコンポーネントがネットワークドライブ上にインストールされている場合、そのアプリケーションの全部分を検出・削除できないことがあります。

ご不明の点は、ソフォス テクニカルサポートへお問い合わせください。

13.16 不要と思われるアプリケーションに関する警告を頻繁に受信する

同じアプリケーションに対して複数のレポートが表示されるなど、不要と思われるアプリケーションに関する警告を頻繁に受信することがあります。

この現象は、一部の不要と思われるアプリケーションがファイルを「監視」し、頻繁にアクセスを試みることが原因の場合があります。オンアクセス検索が有効になっている場合、Sophos Endpoint Security and Control によって各ファイルアクセスが検出され、そのたびに警告が送信されます。

次のいずれかの方法で対処してください。

- アドウェアや不要と思われるアプリケーションのオンアクセス検索を無効にする。代わりにスケージュール検索を実行することができます。
- アプリケーションを認証する (不要と思われるアプリケーションをコンピュータで実行する場合)。詳細は、アドウェアや不要と思われるアプリケーションを認証する (p. 109)を参照してください。
- コンピュータをクリーンアップし、認証していないアプリケーションを削除する。詳細は、コンピュータを直ちにクリーンアップする (p. 54)を参照してください。

13.17 クリーンアップに失敗した

Sophos Endpoint Security and Control がアイテムをクリーンアップしようとして失敗する (「クリーンアップに失敗しました」) 場合、考えられる原因は次のいずれかです。

- 複合型アイテムのすべてのコンポーネントが検出されなかった。残りのコンポーネントを検出するには、コンピュータでシステムのフル検索を実行してください。詳細は、今すぐコンピュータを検索する (p. 53)を参照してください。
- アイテムのコンポーネントが含まれる一部のドライブまたはフォルダが検索から除外されている。検索から除外するアイテムを確認してください (オンアクセス検索の対象から項目を除外する (p. 87) を参照)。リストにアイテムがある場合はリストから削除してください。
- 十分なアクセス権限がない。
- クリーンアップできないタイプのアイテムである。
- ウイルスそのものではなくウイルスフラグメントが発見された。

- アイテムが書き込み禁止のフロッピーディスクや CD 上にある。
- アイテムが書き込み禁止の NTFS ボリューム (Windows) 上にある。

13.18 ウイルスの副作用から復旧する

クリーンアップにより、ウイルスはコンピュータから削除されますが、その副作用は元の状態に戻されないこともあります。

感染による影響をまったく残さないウイルスもありますが、データを変更したり破壊するウイルスもあり、このようなウイルスは検出が困難です。次のいずれかの方法で対処してください。

- 「**ヘルプ**」メニューで、「**セキュリティ情報の表示**」をクリックしてください。ソフォス Web が表示され、ウイルス解析情報を参照することができます。
- オリジナルコピーまたはバックアップを使用し、感染したプログラムを置き換えます。感染前の安全なバックアップコピーがない場合は、将来の感染に備え、作成または入手しておくことを推奨します。

ウイルスによって破壊されたディスクからデータを復旧できる場合もあります。ソフォスでは、一部のウイルスの破壊活動から復旧するためのユーティリティを提供しています。ソフォス テクニカルサポートに問い合わせてください。

13.19 アプリケーションの副作用から復旧する

クリーンアップにより不要と思われるアプリケーションはコンピュータから削除されますが、その副作用は元の状態に戻されないこともあります。

アプリケーションには、インターネット接続の設定を変更するなど OS に変更を加えるものもあります。このような場合、Sophos Endpoint Security and Control がすべての設定を元の状態に戻せないこともあります。たとえば、アプリケーションがブラウザのホームページの設定を変更した場合、Sophos Endpoint Security and Control は変更前のホームページが何であったか判断することはできません。

また、dll ファイルや .ocx ファイルなどコンピュータにユーティリティをインストールするアプリケーションもあります。ユーティリティが、言語ライブラリなど、安全であり (つまり、不要と思われるアプリケーションの要素をもたない)、かつアプリケーションの中核機能でない場合、Sophos Endpoint Security and Control がアプリケーションの一部として検出しないこともあります。この場合、クリーンアップを実行してもファイルはコンピュータから削除されません。

アドウェアなどのアプリケーションは、ユーザーによって意図的にインストールされたプログラムの一部で、プログラムの実行に必要な場合があります。このようなアプリケーションを削除すると、プログラムが停止することがあります。

次の項目を実行する必要があります。

- 「**ヘルプ**」メニューで、「**セキュリティ情報の表示**」をクリックしてください。ソフォス Web が表示され、アプリケーションの解析情報を参照することができます。
- バックアップを使用してシステム設定または使用するプログラムを元の状態に戻します。感染前の安全なバックアップコピーがない場合は、将来の感染に備え、作成または入手しておくことを推奨します。

アドウェアや不要と思われるアプリケーションによる副作用の復旧に関する詳細情報、あるいはご相談は、ソフォステクニカルサポートまでお問い合わせください。

13.20 内蔵ブラウザを使用してアップロードされたファイルがデータコントロールによって検出されない

データコントロールは、スタンドアロン型 Web ブラウザを使用してアップロードされたドキュメントに割り込みます。他社製アプリケーション (例: Lotus Notes など) に内蔵されているブラウザを使用してアップロードされたドキュメントには割り込みません。ブラウザが内蔵されている他社製アプリケーションをご使用で、アップロードされたドキュメントすべてを監視する場合は、外部ブラウザが起動されるよう、同アプリケーションを設定する必要があります。

13.21 アップロードされたファイルや添付ファイルが、データコントロールで検索されない

監視対象アプリケーション (メールクライアント、Web ブラウザ、IM (インスタント メッセージング) クライアントなど) を使用してネットワーク内の場所からアップロードまたは添付されたファイルがデータコントロールで検索されない場合は、ウイルス対策および HIPS ポリシーで、リモートファイルがオンアクセス検索から除外されるよう設定していることが原因のことがあります。この場合、データコントロールに Sophos Anti-Virus オンアクセス スキャナ (InterCheck ™) と同じ除外設定が適用されるため、リモートファイルの検索が無効になっていると、データコントロール機能でリモートファイルがまったくチェックされません。

オンアクセス検索の対象から項目を除外する方法の詳細は、オンアクセス検索の対象から項目を除外する (p. 87)を参照してください。

注
Windows エクスプローラを使用してファイルをコピー/移動した場合、オンアクセス検索の除外設定はデータコントロールに適用されません。この場合、ファイルをリムーバブル ストレージ デバイスにコピーしたり、データを光学メディアドライブに書き込んだりするなど、ネットワークの場所から監視対象ストレージデバイスにファイルを転送しようとすると、データコントロール機能でブロックされます。

13.22 アンインストールしたアップデートマネージャがコンソールに表示される

追加のアップデートマネージャをアンインストールした後も、Enterprise Console の「**アップデートマネージャ**」ビューに表示されることがあります。

アップデートマネージャをコンソールで非表示にするには、アップデートマネージャを選択し、右クリックします。そして、「**削除**」をクリックします。

14 用語集

Active Directory の同期のイベント	Active Directory と同期中に発生するイベント。
アクティブなサブ管理サイト	「グループ」ペインに表示されるサブ管理サイト。
コンテンツ コントロール リスト - 詳細設定エディタ	ユーザー定義のコンテンツ コントロール リストを作成するためのエディタ。コンテンツ コントロール リストは、スコア、最大件数、正規表現、コンテンツ コントロール リストが照合される基準スコアで構成されます。
アプリケーションマネージャ	Sophos Client Firewall でブロックされたアプリケーションの起動を許可、またはそのアプリケーションに対して新しいルールを作成するダイアログボックス。
監査	Enterprise Console の環境設定の変更、ユーザーやシステムによるアクションを監視する機能。
自動保護	Enterprise Console から、Active Directory コンテナ内の各コンピュータにセキュリティ対策ソフトを展開 (ソフトウェアのインストールとポリシーの強制的な適用) すること。
カテゴリ	SophosLabs コンテンツ コントロール リストの分類に使われるタグ。リストは、種類、コンテンツを定義するルール、または適用する地域などに応じて分類されます。
コンテンツ コントロール リスト (CCL)	ファイルコンテンツを示す条件をまとめたリスト。たとえば、クレジットカードやデビットカードの番号、銀行の口座番号、またはその他の個人情報などです。コンテンツ コントロール リストは 2種類あります。1つは「SophosLabs コンテンツ コントロール リスト」で、もう 1つは「カスタム コンテンツ コントロール リスト」です。
コンテンツルール	1つまたは複数のコンテンツ コントロール リストを持つルール。ルール内のコンテンツ コントロール リストすべてにマッチするデータを、ユーザーが特定の場所に転送しようとした際に実行するアクションが定められています。
管理対象アプリケーション	生産性やネットワークパフォーマンスの低下を避けるために、社内で使用すると検出・ブロックされる悪意のないアプリケーション。
管理対象データ	データコントロールの条件にマッチするファイル。
管理対象デバイス	デバイスコントロールの対象となるデバイス。
緊急レベル	アイテムのセキュリティ ステータスが「緊急」に変わる値。

ユーザー定義のコンテンツ コントロール リスト	ユーザーが独自に作成したコンテンツ コントロール リスト。ユーザー定義のコンテンツ コントロール リストを作成する方法は、2とおりあります。1つは、簡単な検索用語リストを作成し、検索の条件 (「このいずれかの用語にマッチ」など) を指定する方法です。もう1つは、コンテンツ コントロール リストの詳細設定エディタを使う方法です。
ダッシュボード	ネットワークのセキュリティ ステータスが一目でわかるように表示されるビュー。
ダッシュボード イベント	ダッシュボードのセキュリティ インジケータの値が緊急レベルを超えるイベント。ダッシュボード イベントが発生すると、メール警告が生成されます。
データコントロール	クライアントマシンからのデータ流出事故を防止する機能。クライアントマシンのユーザーが、データ コントロール ポリシーやルールで指定されている条件にマッチするファイルを転送しようとするとアクションが実行されます。たとえば、ユーザーが、顧客データを含むスプレッドシートをリムーバブル ストレージ デバイスにコピーしようとしたり、社外秘のドキュメントを Web メールのアカウントにアップロードしようとした場合、転送をブロックできます (設定が必要です)。
データ流出防止 (DLP)	「データコントロール」を参照。
データベース	Sophos Enterprise Console のコンポーネント。ネットワーク上のコンピュータに関する情報を保存します。
デフォルトのサブ管理サイト	グループツリー、および「**グループ外のコンピュータ**」フォルダのサーバーのルートノードをルートとして持つサブ管理サイト。デフォルトで、Enterprise Console をはじめて開いたときに表示されます。
デバイスコントロール	クライアントマシンからのデータ流出事故を防止し、ユーザーによる社内ネットワークへのソフトウェアの持ち込みを制限する機能。この機能は、ユーザーがクライアントマシンで認証されていないストレージデバイスや、ネットワークデバイスを使おうとすると動作します。
ダウンロードレピュテーション	インターネットからダウンロードしたファイルのレピュテーション。レピュテーションは、ファイルの古さ、提供元、発生する頻度、詳細なコンテンツ解析、およびその他の特徴を基に算出されます。ファイルが安全であるか、危険で、ダウンロードするとユーザーのコンピュータに害を与える恐れがあるかを判断する必要があります。
管理サイト	「IT 資産」を参照。
除外対象デバイス	デバイスコントロールの対象から明示的に除外されたデバイス。

条件式	「正規表現」を参照。
ファイルのマッチルール	ユーザーが特定の場所に指定されている名前や種類のファイルを転送しようとした場合に、実行されるアクションを指定するルール。例: リムーバブル ストレージ デバイスへのデータベース転送をブロックする。
グループ	Sophos Enterprise Console で定義されている管理対象のコンピュータのグループ。
セキュリティ インジケータ	ダッシュボードのセクションやダッシュボード上のアイテムについて、セキュリティの状態を表すアイコン、またはネットワークの総合的なセキュリティ ステータス。
ホスト侵入防止システム (HIPS)	疑わしいファイル、ウイルス定義ファイルがリリースされていないウイルス、および疑わしい動作からコンピュータを保護するセキュリティ技術。
IT 資産	コンピュータ、ネットワークなどの社内の IT 環境。
Malicious Traffic Detection (MTD)	感染したコンピュータと攻撃者のコマンド アンド コントロール サーバー間の通信を検知する機能。
管理対象コンピュータ	Remote Management System (RMS) がインストールされていて、Sophos Enterprise Console がレポート送信や、ソフトウェアのインストール・アップデートを行えるコンピュータ。
管理コンソール	各コンピュータを集中管理・保護する Sophos Enterprise Console のコンポーネント。
管理サーバー	ネットワークに接続されているコンピュータのアップデート・通信処理を行う Sophos Enterprise Console のコンポーネント。
最大件数	合計スコアとして加算される正規表現の最大一致件数。
最新版のないコンピュータ	最新のソフォス製品がインストールされていないコンピュータ。
パッチ評価	コンピュータにインストールされているパッチ、および未適用のパッチを評価します。
ポリシー	アップデートの設定など、各設定の集まり。コンピュータのグループ (複数可) に適用します。
不要と思われるアプリケーション (PUA)	本質的には悪質ではないものの、一般的に、ほとんどの企業ネットワークには不適切と判断されているアプリケーション。
データ量	ファイルとコンテンツ コントロール リストの照合に必要な最小限のリストキーのデータ型。
データ量のキー	コンテンツ コントロール リストで定義するデータのキー型。「データ量」の設定内容が適用されます。たとえば、クレジット/デビットカード番号を含むコンテンツ コントロール リストの場合、「データ量」で指定した件数を超えるクレ

	ジット/デビットカード番号がファイルに検出されると、コンテンツ コントロール リストが照合されます。
地域	SophosLabs コンテンツ コントロール リストの適用範囲。コンテンツ コントロール リストを適用する国名 (国別のコンテンツ コントロール リストの場合)。すべての国に共通するグローバル コンテンツ コントロール リストの場合は、「グローバル」と表示されます。
正規表現	特殊な文字で表された検索文字列。文字列のパターンマッチに使います。データコントロール機能では、Perl 5 と同じ構文の正規表現が使用されています。
権限	Enterprise Console で特定のタスクを実行するための権限。
ロール	Enterprise Console で許可する操作の権限をグループ化したもの。
ロールベースの管理	ユーザーの組織内の役割に応じて、アクセスできるコンピュータや、実行できるタスクを指定できる機能。
ルートキット	コンピュータのユーザーや管理者から、悪意のあるオブジェクト (プロセス、ファイル、レジストリキー、ネットワークポート) の存在を隠すために使われるトロイの木馬またはテクノロジー。
ルール	ファイルが特定の条件にマッチしたときに実行されるアクションを指定するルール。データコントロールのルールには、ファイルのマッチルールとコンテンツ ルールの 2種類あります。
スコア	正規表現に一致するたびに、コンテンツ コントロール リストの合計スコアに加算される数値。
サーバーのルートノード	「**グループ外のコンピュータ**」フォルダを含む「**グループ**」ペインで、グループツリー階層の最上に位置するノード。
Sophos Live Protection	オンラインベースのテクノロジーを使って、疑わしいファイルが脅威であるかを瞬時に解析する機能。ソフォスのウイルス対策のクリーンアップ機能で設定されているアクションを実行します。
Sophos Update Manager (SUM)	ソフォスのセキュリティソフトとアップデート版をソフォスや他のアップデートサーバーからダウンロードし、共有フォルダに配置するプログラム。
プリセットルール	あらかじめ設定されているルールのサンプル。ソフォスによるプリセットルールの更新はありません。
SophosLabs コンテンツ コントロール リスト	ソフォスが提供・管理するコンテンツ コントロール リスト。SophosLabs コンテンツ コントロール リストは、ソフォスによって更新・新規作成されます。最新のリストは、Enterprise Console からダウンロードできます。なお、SophosLabs コンテンツ コントロール リス

	トの内容は編集できません。ただし、各コンテンツ コントロール リストで「データ量」を設定することはできます。
サブ管理サイト	コンピュータやグループの一部を含む、特定の IT 資産。
サブ管理サイトの管理	処理の実行が可能なコンピュータやグループを制限する機能。
ソフトウェアのサブスクリプション	様々なプラットフォーム用のソフトウェアバージョンの集まり。ユーザーが選択し、Update Manager によってダウンロードされ、常に最新の状態に保たれます。Windows に「Recommended」を指定するなど、対応プラットフォームごとに 異なるバージョンを設定できます。
疑わしい動作の検知	システム上で起動している全プログラムの振る舞いの動的な解析。悪意があると思われる動作を検知・ブロックします。
疑わしいファイル	ウイルスによく見られる特徴を持ちながらウイルスに限定されない特徴も持つファイル。
同期の頻度	Enterprise Console の同期ポイントを選択した Active Directory コンテナと同期する間隔。
同期ポイント (Active Directory ツリー用)	同期をすることによって、選択した Active Directory コンテナの内容 (グループとコンピュータ、またはグループのみ) が追加される Sophos Enterprise Console のグループ。コンテナの構成は保ったまま追加されます。
同期: Active Directory との同期	Active Directory の組織単位 (OU: Organizational Unit) またはコンテナを Sophos Enterprise Console のグループへ一方向同期すること。
同期したグループ	同期ポイントより下方に位置するグループすべて。
システム管理者	ネットワーク上のソフォスのセキュリティソフト、および Enterprise Console のロールを管理するために、あらかじめ設定されているロール。フルコントロール権限が与えられています。 システム管理者ロールは削除もすることも、その権限や名前を変更することもできません。また、このロールから Windows のグループ「Sophos Full Administrators」を削除することもできません。他のユーザーやグループは、このロールに追加したり、削除できます。
タグ	SophosLabs コンテンツ コントロール リストが持つ記述子。コンテンツ コントロール リストの内容や適用範囲が記されています。タグは 3種類あります。タイプ、規約、および地域です。
タンパー プロテクション	既知のマルウェアや未認証のユーザー (ローカル アドミニストレータや専門知識のないユーザーなど) が、ソフォスのセキュリティソフトをアンインストールしたり、Sophos Endpoint Security

	and Control の GUI を通じて無効に設定することを防止する機能です。
しきい値レベル	アイテムのセキュリティステータスが「警報」または「緊急」に変わる値。
合計スコア	コンテンツ コントロール リストの内容にマッチすると加算されるスコアの合計。
基準スコア	正規表現のマッチ回数。この値を超えると、コンテンツ コントロール リストが照合されます。
判定ファイルタイプ	ファイル拡張子にかかわらず、ファイルの構造を解析することによって判定されたファイルタイプ。より信頼性の高い方法です。
タイプ	SophosLabs コンテンツ コントロール リストの分類タイプ。たとえば、パスポートの内容、住所、またはメールアドレスを持つコンテンツ コントロール リストは、個人情報として分類されます。
アップデートマネージャ	「Sophos Update Manager」を参照。
警報レベル	アイテムのセキュリティステータスが「警報」に変わる値。
Web コントロール	社内の Web アクセスポリシーの設定、施行、および Web 閲覧履歴のレポート表示を行う機能。特定の Web カテゴリの閲覧を許可またはブロックしたり、ポリシーに違反する Web サイトを識別し、ブラウザに警告を表示したりできます。
Web Protection	Web ページに存在する脅威を検出する機能。この機能は過去に悪質なコンテンツを含んでいたことのある Web サイトをブロックしたり、悪意のあるダウンロードを防止したりします。Web Protection 機能は「ウイルス対策および HIPS」ポリシーに含まれています。

15 テクニカルサポート

ソフォス製品のテクニカルサポートは、次のような形でご提供しております。

- ユーザー コミュニティ サイト「Sophos Community」(英語) (community.sophos.com/) のご利用。さまざまな問題に関する情報を検索できます。
- ソフォス サポートデータベースのご利用。www.sophos.com/ja-jp/support.aspx
- 製品ドキュメントのダウンロード。www.sophos.com/ja-jp/support/documentation.aspx
- オンラインでのお問い合わせ。 https://secure2.sophos.com/ja-jp/support/contact-support/support-query.aspx

16 利用条件

索引

い

う

え

お

く

こ

さ

し

す

せ

そ

た

ち

つ

て

と

ね

は

ふ

ほ

め

ゆ

ら

る

れ

ろ

わ